EMERGING TECHNOLOGIES:

Recommendations for Counter-Terrorism

Edit Volume

January 2001

Edited by:
Joseph Rosen, MD
Charles Lucey, MD, JD, MPH

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
DARTMOUTH COLLEGE

EMERGING TECHNOLOGIES:
Recommendations for Counter-Terrorism

Edited by:
Joseph Rosen, MD
Charles Lucey, MD, JD, MPH

January 2001

Institute for Security Technology Studies
Dartmouth College
Hanover, New Hampshire

ACKNOWLEDGEMENTS

Many individuals helped make this effort and the resulting publications possible. Of course, all of the conference and paper contributors deserve the real credit for the ideas in this document. Dean Lewis Duncan provided the inspiration for undertaking this project. Mr. D Arcy Morgan of the National Institute of Justice, and Mr. Robert Greenberg of GH International provided useful guidance. I m indebted to Dr. Richard Scribner, Acting Director, ISTS for his guidance and support throughout this project. Ms. Nicole Hall Hewett provided enormous logical, organizational and publications support. We couldn t have done it without her. Ashley Tanner and Ann Marion also provided invaluable support.

Joseph Rosen, MD
January 2001

Institute for Security Technology Studies
Dartmouth College
45 Lyme Road, Suite 200
Hanover, NH 03755
Tel: (603) 646-0700
Fax: (603) 646-0660
www.dartmouth.edu/ists

CONTENTS

Foreword

Terrorism as a threat to America is growing both domestically and internationally. America no longer has fixed borders either geographically, politically, economically or in cyber-space. Therefore we cannot defend ourselves from this threat using older unresponsive, dated, merely reactive conventional methods. As threats change, we must change our response to these threats. Technology will play a key role in predicting, monitoring, responding to the full spectrum of threats in the 21st century.

Our mission is to assess emerging technologies that may present as new threats to America's security, we also see other emerging technologies as possible cures for these threats. A cure may be seen either as a tool to prevent a threat or to treat its consequence. As a physician I have a specific viewpoint which often looks at a threat as a disease, and a new technology as a treatment. Other similiarities exist as well when we deal with both biothreats and cyberthreats. Their method of attack is similar in the sense that they infect and spread. They have many more similarities that we will deal with in this report. Most importantly, they both have the capability of being a strategic threat to America.

We have assessed emerging technologies from both the offensive and defensive point of view. Although we initially thought to limit our report to only emerging technologies, our report is framed in the context of present and future strategy and operations that America will use to fight terrorism. From meetings with people from the areas of policy, operations and from technology we found that we learned most from the process that occurs at the intersection of these three areas. We also found it to be clear that there existed a need for emerging technologies to be used to integrate the interaction between these three groups.

We believe that we can contribute in this report to our basic knowledge about emerging technologies - both as threats and treatments (response and solutions). But we also believe that our recommendations need to address how to evolve our policy, operational plans and technology together. In this report we have included key papers and comments on strategy and operations as a framework for how we believe we can protect our society in the 21st century from terrorist attacks. We have also listed other comprehensive reports that create a body of knowledge that is critical to an understanding of the present and future environment of terrorism and counter-terrorism efforts.

In our project we have limited ourselves to an attack that combines cyber and bio, because the methods required to prevent or respond to a combined cyber and bio attack will more than likely cover what needs to been done to respond to other attacks whether they include explosives or other weapons of mass destruction. A bio threat was specifically chosen as an area of study because of its low cost, its large scale of casualties, its reliance and effects on the medical responder and its ability to spread rapidly and become a strategic weapon. It is both our newest threat, and it is historically one of our oldest threats.

As background to our efforts on emerging technologies we reviewed the present strategy and policy of the US. We also reviewed the federal response plan and multiple state plans that were available to us. We found that our strategy and policy must be based on a 21st century view of America as a country without physical or virtual borders. This includes operational plans based on a sound strategy that allows first responders, FBI, FEMA, DHHS, DOD and other state and federal agencies to work together to prepare for, detect and ultimately to respond to an attack. Emerging technologies will play a critical role in this response. They will also play a critical role in permitting terrorists and their groups to cause potentially greater harm to our society. In the past this harm has been limited to a tactical threat, in the future as incidents of terrorism as well as our response escalates we may cross a threshold and be faced with strategic threats such as the large-scale use of bioweapons within the Continental US.

This report provides specific recommendations for a process that will prepare the U.S. for this eventuality. This report will also describe how emerging technologies could create a system to prevent an attack through improved intelligence. It will also present emerging technology that could limit the extent of damage of a mass casualty strategic bioweapons attack on America.

In summary we present a timeline for future threats from weapons of mass destruction, especially bioweapons. This timeline will cover from the near term to the year 2025. We present one major recommendations for how to prepare for these threats. The recommendation involves the use of virtual reality in the form of a large-scale distributed simulator that will be used to evaluate alternate reponse strategies, technologies, and evolve into a fielded national distributed command and control system. Other recommendations to enhance response preparations are included.

Many limitations exist in any report on terrorism. We have tried to accomplish as much as possible with the help of many individuals. If implemented we believe that this report will provide a number of recommendations that will help to protect our society from the growing threat of terrorism. I would like to thank everybody that have generously given their time and support in the preparation of this product.

Joseph Rosen, MD

Mission Statement

The Institute for Security Technology Studies at Dartmouth College was awarded a grant by the Department of Justice, National Institute of Justice to perform an assessment of emerging technologies. These technologies may affect our national security either as potential threats or as tools of counter-terrorism. These tools may be used as methods of prevention or as part of an overall response plan to terrorist attacks.

Terrorism is defined by the FBI as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any state, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives. Terrorism, in the past, has generally used explosive, conventional weapons as their tools for creating violent acts. In the future, it is expected that this may escalate to the use of weapons of mass destruction and casualties. These weapons may include nuclear, chemical, biological, and/or cyberthreats. In our report we concentrated on a combined bio and cyberthreat to emphasize a specific type of attack.

This attack would be different than previous terrorist attacks, or future potential nuclear or chemical attacks, in that it would present an attack that could be of strategic consequence to America s security. It would be an attack that if not prevented, or contained, would spread rapidly throughout our society both geographically and within cyberspace. This type of attack would also allow us to study what process is needed to prepare us for any type of attack from a weapon of mass destruction, or from an attack with conventional weapons that involved multiple sites, or one sustained over a period of time. This approach has given us a unique opportunity to provide recommendations, and a system that could provide a simulation environment in which we could prepare for any number of terrorist attack scenarios in the future. This simulation environment is a key recommendation of our report and could be used to prepare, potentially prevent, and train for a response to a large-scale strategic attack from a weapon of mass destruction. It could also be used to implement an augmented reality system that could be used to coordinate a large-scale tele-operated remote response to an overwhelming attack from a weapon of mass destruction, such as a bioweapon.

In approaching our task, we emphasized emerging technologies from the present through the future. We specifically looked at 2000, 2005, and 2025. We included first responders, both from the law enforcement and the medical community. We included operators from the crisis and consequence communities. We also included policy makers in our conferences and individual meetings. We brought these groups together with leading technologies from many areas of emerging technologies. These technologies, in many cases, had a double-edged sword in the sense that they could be used for both threats and responses. We emphasized recommendations that we obtained through extensive discussions with these groups and individuals.

What we have found to be the unique challenge is the process necessary to unite policy makers, operators, and technologists into a common framework to rapidly change in the face of emerging threats. Our present strategy and policy must respond to new threats that are brought on by the introduction of inexpensive weapons of mass destruction such as bio weapons and cyberthreats. These affect our policy decisions. Our policy then directs our operational plans. The changes in our operational plans often require the introduction of new emerging technologies to meet the demands of new threats. Then the cycle is repeated with the introduction of new threats. This cycle is increasing in its tempo as we enter the 21^{st} century, and our ability to respond to this need to evolve and change is critical to the protection of our institutions, whether it be our physical or cyberspace infrastructure.

We found a need early in our mission to address how emerging technology influences this cycle of terrorism/counter-terrorism policy, operations, and emerging technology. Although we have many recommendations regarding responses to specific threats with specific new technologies, we have found our over-arching recommendation to be a central technology that would allow each of the groups, agencies, and individuals involved in creating our response to terrorist threats to have a process that would enable them to more rapidly adapt to this challenge.

Our key recommendation is a process based on emerging technologies that will enable the US to more rapidly respond to emerging threats from terrorists, especially if these threats move from conventional explosive devices to weapons of mass destruction. This process involves the use of virtual reality in the form of a large-scale distributed simulator that brings together policy makers, crisis and consequence operators, and technologists. This will enable each of these groups to participate in a realistic manner through a large number of scenarios and test our new approaches to meet the challenge of terrorism. It will also allow us to determine if a given policy and its implementation result in a favorable outcome, or an escalation in the terrorist response. These simulation tools have been used successfully in the past by both the civilian and defense communities to train and prepare for unusual events. This tool could play a key role in training and preparation in our efforts against terrorism.

This same large-scale distributed simulation environment will provide the infrastructure for more than just a training environment. It will also help to predict the outcomes of our responses to specific scenarios. In many cases it may reveal that a response to a specific attack may cause an inversion, in which what we believed to be right policy choice may lead to future escalation of violence, or immediately to an increase in casualties. This may be especially true in attacks where the site is contaminated, such as is the case with biological weapons, and with nuclear and chemical attacks.

Finally, the infrastructure created through this large-scale virtual reality simulator may be used in the prevention of terrorist attacks, or directly in the implementation of a response to a specific attack. Performance machines are augmented reality systems that combine a virtual model of a situation superimposed on the real events. They are used in surgical simulators and in teleoperations in remote areas. Teleoperations may be used in law enforcement for defusing bombs, in industry for a response to a contaminated zone, or in deep-water rescue missions. This technology is ideal for a response to a large-scale terrorist event in which there are mass casualties and the resources needed are either not available locally or the use of local responders will endanger their lives. This system would allow the coordination of crisis and consequence management from multiple remote sites to provide the necessary support in a timely manner to the sites under attack. For this to work effectively it would first need to be practiced in a large-scale simulation environment. We need to prepare for large-scale events prior to the events occurring, so that we can minimize our casualties and protect our society from both tactical and strategic threats from weapons of mass destruction.

It will be the mission of this report to explain how emerging technologies can be used to respond to terrorist threats in the 21st Century from weapons of mass destruction and conventional weapons. It will also be the mission of this report to provide insight into what emerging technologies we expect will become available to the terrorist community in the future. Although we hope that weapons of mass destruction do not become a tool for terrorists, we have seen a trend over the past ten years with an escalation in not the number of events, but in the scale of casualties from these events. We need to prepare at several levels to address this trend, and to protect America from emerging technologies that may threaten our society and critical infrastructures whether they are physical ones or part of our cyberspace.

Joseph Rosen, MD

Biological Terrorism Emerging Threats Assessment: Response Recommendations

Introduction

The U.S. Department of Justice, National Institute of Justice, tasked the Institute for Security Technology Studies at Dartmouth College to make response planning recommendations, as part of its grant to study emerging terrorist threats. The July 7-9, 2000 Conference on Biological Terrorism developed ideas presented by conferees, based on Dr. David Franz's white paper and other submissions. These were further reviewed and refined at a September 23, 2000, Ad Hoc Advisory Group meeting in Washington, DC.

The Institute for Security Technology Studies Emerging Threats Assessment Program response recommendations cover these twelve areas:

1) Technology Base: Research and Development
2) Intelligence and Surveillance
3) Medical Countermeasures
4) Physical Countermeasures
5) Forensics
6) Proactive Deterrence
7) Public Health Infrastructure
8) Interagency Collaboration
9) Education
10) Complementary programs
11) International Cooperation
12) New Technologies

Central to the recommendations are the following: (1) we must prepare for hundreds to thousands of casualties; even if the current probability of attack is low, it will certainly increase with the dissemination of scientific advances, possibly to the point of empowering of the individual terrorist; (2) there must be a concerted effort and investment with strong leadership to improve preparations in the years ahead; and (3) most investments and new technology applications will have a beneficial dual use -- for our public health structure and for our society.

Summary

1. Technological base: multi-year appropriations for biological terrorism basic science research should fund public and private efforts to achieve practical defensive applications. We believe that we understand the relative limits of nuclear physics and chemistry, but we do not understand the limits of biology -- for good (medicine), or for evil (biowarfare). The future biological warfare or terrorism threat is relatively unknown; therefore, it will be difficult, especially in the medical arena, to prepare specific countermeasures for all threats. We must be capable of responding quickly and effectively to the unknown; therefore, our technical base must be deep and broad.

There is not a military-industrial complex for biological defense as there was for our nuclear weapons and energy programs. We must strengthen our military tech-base for threat evaluation, pathogenesis, and specific medical countermeasures research. We must expand and leverage non-military government public health research, especially in the areas of immunology, diagnostics and drug development. We must increase our support to academic research, and partner with the pharmaceutical industry for advanced development and production of orphan vaccines and antiviral drugs. All of these efforts will provide more spin-off application to public health than we typically expect from defense research. Finally, we must demonstrate that we are in this battle for the long term. Multi-year research grants can help assure completion of technology objectives.

2. Intelligence: human covert intelligence gathering, electronic communication and Internet monitoring, and advanced data mining must be continually interpreted and refined through computer simulation and "red teaming (opposing teams expert event exercises)" to proactively anticipate future threats. Intelligence for bioterrorism is extremely difficult because of the dual-use nature and minimal signature of weapons programs. Facilities, equipment and human resources for the R&D and production of biological agents are not unique. Even weaponization and dissemination---especially for the terrorist---can be done with equipment stolen from legitimate industry. Precursors are not unique, and signatures are non-specific, rapidly diluted or destroyed in the environment, or nonexistent. Maintaining quality expertise in our intelligence analyst corps is proving difficult because of competition from industry for our best young scientists...and because of mundane aspects of the analyst's job. On the other hand, the "new openness" fostered by information technologies and the spread of free enterprise biotech throughout the world offer new options for information data mining. We must not only use these technologies to better understand the threat worldwide, but to better use human sources that are more plentiful in the era of increased mobility. Excellent intelligence is key for early threat detection to gauge intent and capabilities and to perform proper threat assessment. While sources and methods producing intelligence are often classified, the products of a rigorous intelligence program can facilitate both deterrence and response on the streets of our cities.

Scientific methodology must be applied to the study of terrorism, to develop better theories regarding the "seeds of terrorism," to improve psychological profiling of terrorist groups, and to understand how past events may be a prologue to future events. For example, what lessons may be applied from knowing that former CIA-trained Afghan freedom fighters joined terrorist groups and that a former U.S. serviceman was convicted for the Oklahoma City bombing? What political or operational decisions made today may impact our future? How might we have avoided the recent attack on the USS Cole? Should we require "terrorism impact studies," as we now require environmental impact studies? Might some of the information sharing that Radio Free Europe used to fight the iron curtain now be turned to fighting cultures fostering terrorists through internet and broadband technologies?

3. Medical countermeasures: just as the US has a National Cancer Institute (NCI, under NIH) to coordinate and sponsor anti-cancer research, there needs to be a focused effort to equip and update America's cities (the para is quite a bit broader than just a first responder focus) with tested and proven vaccines, drugs, laboratory tests, treatments, and so forth. Protecting civilians from bioterrorism is more difficult than protecting a military force. For the force, we can use: (1) active immunization for some agents; (2) passive immunoprophylaxis and chemoprophylaxis for others; (3) battlefield detection systems; (4) physical protection (masks); (5) identification and diagnostic tools and methods; (6) decontamination procedures; (7) passive immunotherapy; and (8) chemotherapy. For an attack on our citizens, our useful countermeasures begin with identification and diagnostics and essentially end with chemotherapy (medical treatment).

Identification of the agent used in an attack is of critical importance. Without this, rational post-exposure prophylaxis will be futile. Diagnostic capabilities must be ready in the field, throughout a network of hospital and government clinical laboratories, and in key national reference laboratories. Classical and molecular methods must be known and validated. Triage may be critical to success in therapy for the right subpopulation. Humans exposed, even to replicating agents, may not have measurable amounts (by current tests) of the agent in their blood or serum for several days at the earliest, nor will they have a measurable immune response. Yet, humans -- or domestic animals -- may be the only sentinels at the site of the aerosol attack. Therefore, methods of preclinical diagnosis and triage tools must be developed.

We must stockpile sufficient antibiotics effective against anthrax, pneumonic plague and tularemia (as in the CDC's National Pharmaceutical Stockpile Program). Prolonging the shelf life of the antibiotics could facilitate this. Today, neither antiviral drugs for smallpox nor vaccines for the two agents -- smallpox and anthrax -- for which they might be needed post-attack, are available in sufficient quantities to allow stockpiling. We must leverage industry and academic research for antiviral drugs that target selected threat-agent active sites. We must develop adequate stocks of anthrax and smallpox vaccines. Most experts believe that ventilators are likely to be in short supply after an attack on a city, with certain of the most lethal classical agents. We must also prepare for rapid acquisition of necessary equipment and hospital bed space in an emergency. Finally, we must consider and prepare for the potential psychological impact of a biological attack on a society frightened by novels, movies and media spin.

Further thought and planning need to be done for a national medical response plan that could rapidly be deployed in the face of a biological attack affecting 1% or more of a city's population. The recent terrorism rehearsal ("TOPOFF") in Denver, demonstrated severe strain and burnout when relying primarily on the medical and nursing staffs of local hospitals. There is a need for a national consensus on a biological response strategy allocating response preparedness, to avoid this outcome in the future.

4. Physical countermeasures: continuing efforts to improve biosensors to protect public areas must be encouraged along with development of other defensive measures such as inexpensive face masks. Fewer physical countermeasure options exist for the civilian population than for the military force. At present, technological hurdles (cost, logistical requirements, narrow spectrum and high false-positive rates) prevent the widespread application of sensor technologies for biological terrorism. We lack the accurate, self-validating, dynamic sensors that are necessary to avoid false positive alarms. A clearer delineation of current sensor capabilities versus the real threat, and an independent test center to test and certify equipment would be useful. Without timely warning, protective masks seem to have little utility. However, some experts advocate the development of a simple, inexpensive "bio-only" mask to be carried in automobile, briefcase or purse. To date, this concept falls below the threshold set by the balance between perceived risk and benefit to the population. Collective protection by modification of HVAC (heating, ventilation, and air-conditioning) systems in critical public buildings may have utility. Decontamination of patients, buildings and environmental areas should be considered. It is believed that decontamination following a biological event is less important than following a chemical attack. The true aerosol that is required for effective dissemination of the non-volatile biological agent might leave little residual, except around the area of detonation. The agent deposited is thought to be poorly reaerosolized and subject to inactivation by environmental factors, especially ultra-violet light.

5. Forensics capability: as we invest money to develop better tests and procedures, we must also validate them so that we can rely on these experts when making national military responses or in courts of law. While diagnostic capabilities are paramount in responding medically to an attack, attribution following a bioterrorist attack will require exquisite forensics capabilities. We must be capable of quickly dissecting an organism at the molecular level. More importantly, people who are familiar with the epidemiology and laboratory characteristics of strains and isolates from around the world, and who work with these agents daily, must do this work. Obtaining the complete genetic fingerprint of an agent used in a biological attack may be a crucial clue for attribution. It may tell us if this is a natural strain or a bioengineered agent. Forensics may hold the key to determining whether an outbreak is a natural or manmade event. Even in preparation, what we learn about the genomes of the biological agents of concern will have application in basic science and public health.

6. Proactive deterrence: this is a vigilant posture that uses all tools and tactics at its disposal to aggressively deter and preempt biological terrorism. We must remain alert and aware, never letting down our guard. We must employ all means, including diplomacy, intelligence, detection, prosecution, and sanctions when indicated. This may also require a political will to retaliate, which is clearly understood by anyone contemplating such violence (with due respect to U.S. and international law). The way we respond to the first use of biological agents against our citizens, even if it is not a mass-casualty event, will likely set the general course for our future interplay with the biological terrorist. The Israeli model for defense against airline hijacking -- granted a less complex problem than we face here -- has proven effective: vigilant, integrated, uncompromising and swift. We must take the most extreme measures against known proliferators and users of biology to harm our citizens; their clear understanding of our resolve will serve as a deterrent.

7. Public health infrastructure: these are our medical first responders, our medical first line of defense; recent outbreaks like AIDS, West Nile Virus, and Ebola Virus illustrate how important public health personnel are to future response preparation. Strengthening our public health infrastructure should be at the forefront in our preparation for defense against bioterrorism. Effective surveillance programs, improving the laboratory capabilities at state and local levels, teaching and practicing public health and epidemiology, and enhanced communications and health threat response systems are all dual-use functions. Not only do they prepare us to better respond to a human-made outbreak, but to naturally occurring ones as well. The CDC and state health departments must continue to improve their information networking and sharing. We must develop surveillance systems that can differentiate a slightly increased incidence of disease from "normal" expected disease rates, yet protect the confidentiality of patients. The current initiative supported by the Public Health and Social Services Emergency Fund for FY2000 is an important start. As with our biomedical tech base and intelligence programs for biodefense, we must think "long-term" in supporting our public health infrastructure. It will be cost effective.

8. Interagency collaboration: this can only be improved by strong leadership/structure, supported by computer simulation exercises and actual practical exercises, to keep the various state and federal agencies in sync and ready for the future. Preparing to respond to biological terrorism must involve intelligence, law enforcement and other traditional emergency responders, clinical and research medical communities, public health, political leadership and the military. It must involve national, state, regional and local organizations, agencies and officials. As the perceived threat has mounted and the federal government has responded with funds, bioterrorism defense has become a growth industry. Yet, no single office with the necessary authority has clearly taken the lead, either within the Department of Defense or within the federal government. Therefore, interagency collaboration has become even more important. Vertical (local through national) and horizontal (across all disciplines) communication and willingness to collaborate are imperative. Excellent leadership facilitates necessary collaboration. Serious consideration should be given to selecting a single lead coordinator, possibly modeled on the "Drug Czar." Strong central leadership could seamlessly integrate command, control, communications, computer systems, and intelligence operations, perhaps following a military organizational model with additional responsibility for coordinating medical care for massive casualties that overwhelm local resources. (Some conferees were satisfied with current federal plans to use the FBI -- a lead federal agency for crisis management -- and FEMA as lead federal agencies for consequence management). Virtual reality computer simulation technology could aid command and control preparation and training.

9. Educational programs: just as investment in education has contributed to making us the world leader in technology, it can also benefit the unique field of bioterrorism defense prevention. Education and training must be given the highest priority. The fundamental need in a hospital or medical center facing a spike in the patient load following an attack is application of the standard principles of medicine with which the professional and support staffs are already intimately familiar. However, our health-care providers have not seen the diseases caused by many of the threat agents. Education and training must include the general characteristics of biological agents versus chemical agents; clinical presentation, diagnosis, prophylaxis and therapy of the most important diseases; sample handling; decontamination and barrier patient care. Training, planning and drills must prepare physicians and first responder staff for mass-casualty patient management, respiratory support for unusual numbers of patients, distribution of medications and support of the local government in vaccination programs. Engineering staffs must be taught to establish improvised containment in patient rooms or suites. Traditional emergency-responders and public and military leaders must understand rather complex technical and biological issues in order to effectively balance cost and benefit in preparation and response. Application of the knowledge we already have though education may be the least expensive and the most important thing we can do as we prepare. There is a need to develop educational modules for professional schools of medicine, law, and engineering. Special educational efforts should be made for federal and state elected officials. The conferees urge DOJ to seek sources of funding to dedicate to these efforts. There is a need for one group to be responsible for monitoring new technology and information in order to bridge the knowledge gap with emergency responders, so as to keep them fully aware of new threats, technologies, etc.

10. Complementary programs: we must continually support and seek out less obvious or direct programs as partners in this war against bioterrorism. In addition to the obvious domestic preparedness initiatives needed, we must continue to be prepared through the military (available to assist the FBI upon request under current federal plans) or law enforcement, to destroy biological weapons whether deployed or in storage. We must have the means to neutralize facilities wherever they are found. We must seek and support international law that would bring proliferators to justice. We must seek to enhance communication between scientists internationally, through cooperative threat reduction programs with states that might threaten us; there are significant risks inherent in these programs, but there are huge potential payoffs as well.

11. International cooperation: the fight against terrorism must be worldwide, coordinated, and ongoing, with every attempt made to resolve potential conflicts that could result in future incidents. While U.S. efforts to strengthen domestic biological warfare response capabilities and preventive measures are well founded and need expansion, we should consider biological terrorism a global problem. First, terrorists with biological weapons could emanate from any part the world and attack U.S. assets at home or abroad. Furthermore, biological terrorists incidents elsewhere in the world would impact American society by adversely affecting the international economy and our own sense of security. A holistic global strategy to prevent and to respond to biological terrorism is needed not only to determine what could be done internationally to strengthen prevention, but to lay the groundwork for enhanced international cooperation to this end. (There is benefit in tracing certain individuals and organizations across boarders.) Currently we tend to look at the problem of biological warfare primarily through our own perspective, though we are cooperating with Britain and Canada on WMD issues. [Actually, we are also cooperating with some others. We could generalize and say "cooperating with allies on WMD issues"] There is every reason to believe that an international effort to identify integrated ways to prevent and respond to biological incidents would yield new and valuable approaches to deal with the problem. Such a perspective would also allow the U.S. to better focus its internal measures in light of a global strategy.

12. New technologies: these must be assessed for potential bioterrorism defensive and offensive capabilities. We must exploit to the fullest, the phenomenal advances in both biotechnologies and the cyber- and communication technologies that have occurred in parallel with the changing biological terrorist threat. Genomics and proteomics are revolutionizing diagnostics, vaccine development and drug discovery. These have obvious and wide application for biodefense. Telemedicine, robotics, virtual reality and simulation, nanotechnology and the Internet and wireless communications must be used to replace or augment human capabilities and allow us to respond more quickly when lives are threatened. If we keep the pressure on those who would use these breakthroughs for evil -- taking away their freedom through effective intelligence programs and law enforcement -- we will be more likely to stay steps ahead as we use the technologies for good, and provide an additional deterrent to the threat. It would be useful to have a lead group to evaluate new emerging technology, sponsor research and development, and commercialize proven new technology. Potential future threats go beyond currently considered pathogens and approaches. As a simple example, binary biological threats of the future might require a priming agent followed by a second agent (e.g. a vitamin or antibiotic) to initiate a viral infection or cancer. New weapons technologies will require a dynamic and responsive approach to domestic preparedness.

Conclusion

Participants in the Program on Emerging Threats Assessment believe that ongoing efforts such as the Dartmouth College July Conference should be a national priority to regularly update developments in the area of biological terrorism. A majority agreed that scientific advances, if not already impacting existing offensive capability, will be more available and applicable over the next 5 to 25 years. Preparation for biological terrorism affecting agriculture and industry was also urged. The potential for cyberterrorism to be used in conjunction with a biological event was also held by some participants to be a present danger meriting further research. It will be critical for present and future technologies to be applied to response planning. Computer simulators, telemedicine, and robotics were identified as current technologies that could be added to response planning over the next 5 years to radically improve our capability to handle such an event. Over the next 25 years, emerging technologies such as nanotechnology and computer informatics should improve our detection and response capabilities. Investment, coordination, and leadership are critical to this effort to defend against the poor person's nuclear weapon.

Policy in a Borderless World in the 21st Century— The Role of Emerging Technologies

Joseph Rosen, MD

The mission of this report is to assess the impact of emerging technologies on terrorism. The connection between technologies and policy can take many forms. The clearest of these is the influence of emerging technologies that create new threats that will, in turn, influence our policies. Emerging technologies will also create new tools that will help us prevent and respond to terrorist threats. In sum, the technologies will impact both our policy and our operational plans; and given that these changes may affect the US more than other countries, there will be profound effects on our policy and strategies as a nation.

Strategy is an evolving process that incorporates quantifiable objective factors, and factors that are unquantifiable and subjective. Operational plans can only succeed when based on good strategy and policy. If our policies are not adjusted to the realities of a borderless world in the 21st century, our operational plans will not be capable of responding effectively to new threats.

Biothreats and cyberthreats inherently are ideal weapons in a borderless world. A world that is shifting from distinct borders to a global environment — both with respect to our physical borders for biothreats, and to our borders in cyberspace for cyberthreats. They both easily cross their respective physical- and cyberborders. They are relatively inexpensive compared to explosive, nuclear, and chemical weapons with respect to the damage they can cause. Most importantly, they can replicate themselves and spread again across borders in their respective worlds. They, in some special cases, will be strategic weapons and could potentially undermine the very fabric of our society.

The US counterterrorist policies are based on what we believe to be a rapidly shifting trend in global terrorism. (Patterns of Global Terrorism 1999 — United States Department of State —April 2000). This trend is based on a shift from state sponsored international terrorism to "loosely organized, international networks of terrorists." We have made strong efforts to eliminate the safehavens in which these terrorists and their groups operate. This policy is based on a notion that we can in the future isolate terrorists and create a boundary between their threat and ourselves. This is even more difficult with respect to domestic terrorist organizations, groups, and individuals. In the 21st century emerging technologies have made it very difficult to keep our borders safe, whether these borders are physical or in cyberspace.

Strategy and policy are based on variables that are often unique to each nation. These include geography, history, economic factors, the organization of government and military institutions, and finally religions, ideology and culture. The modern US has very unique factors compared to many other nations. Although we will not go into all of these factors, a key factor we will emphasize is geography. It is through geography that we will show how dramatically the landscape of the 21st century will be altered from our 20th century position. Many of these changes have already been put into place, more will come by 2005, and by 2025 we expect that dramatic changes will have occurred that will severely stress our ability to protect our borders and at the same time preserve our present position in the world.

With the fall of the Berlin Wall, and the end of the Cold War, we have seen a shift to a borderless world in which boundaries, walls, and isolation are more difficult to achieve.
For almost one-half century we had strategies and policies based on a world of definitive borders. These strategies and policies may no longer be valid. Information technologies played a key role in removing this wall even before it was physically torn down. Biotechnologies have created weapons that easily cross our physical borders, just as information technologies have created weapons that easily cross our cyberspace.

This transition from a world with borders to a world without borders affects both our physical world and the world of cyberspace. Although we would like to base our strategy on creating a border between ourselves and our threats, this notion of isolation geographically, and isolation within cyberspace may not be an achievable goal in the 21st century. We may apply many technologies to achieve a safe and secure border but emerging technologies that penetrate this wall will continue to advance more rapidly than our emerging technologies to respond to them.

Presidential Decision Directives 62 and 39 can be summarized as the US policy of counterterrorism:

Our policy has four main elements:

- First, make no concessions to terrorists and strike no deals
- Second, bring terrorists to justice for their crimes
- Third, isolate and apply pressure on states that sponsor terrorism to force them to change their behavior
- Fourth, bolster the counterterrorist capabilities of those countries that work with the United States and require assistance"

We believe that this is a strong policy and operationally is being increased to encompass the threat of weapons of mass destruction. However, key to this policy is a world with borders. America s policies have been heavily based on the ability to isolate an enemy and defeat them offshore or in their own homeland, not within the continental US.

Geographically, we have been isolated and protected from direct attack. Our defense has been based on our isolation with the Atlantic Ocean on our east and the Pacific Ocean on our west. We have not been faced with invasion, but have been able to fight our wars on the sea or on distant shores (George Baer, Strategy 1890-1990). We have been protected by our military through a strong Navy, Army, and more recently, air superiority. In the 21st Century the global environment requires new strategies and policies to effectively control an enemy that is transnational and is willing to use terrorist means, including weapons of mass destruction, to achieve their goals.

Technologies that were once expensive and only available to a few are now inexpensive and ubiquitous. This has created both a cyberspace and physical space that the US shares with other nations, groups, and individuals. With the loss of this geographic isolation, we will have to dramatically alter our policy and strategy to effectively protect us from new weapons based on emerging technologies that can be disseminated widely and cross our old borders with impunity.

We have included an overview paper on US policy in the future by Rafael Perl. Also included in our reading list is reference to a Report to Congress on International Terrorism: A Compilation of Major Laws, Agreements, and Executive Documents, dated July 2000 (Patterns of Global Terrorism 1999 — United States Department of State — April 2000). In addition, we have referenced other recent documents for review. We also recommend the National Committee Report on Terrorism that reveals a trend to more violent attacks with a greater number of casualties.

In our edited volume we have included a number of papers from the congressional research service. These papers chronicle a decade of escalating events in terrorism. They include coordinated attacks and attacks on strategic targets. The attacks show no boundaries with respect to whether they attack the US on foreign soil, in transit or in the continental US. At some point a threshold may be reached where our present policies will not protect us from the use of a weapon of mass destruction.

The goal of this report is to create a process that will enable policy makers, operational players, and technologists to work together to evolve a strategy that may reverse this escalating trend. This is not to say that there are not effective present methods to accomplish this. It is to say however that emerging technologies in virtual reality and training can be used in new ways to address this issue of counterterrorist policy and strategy and connect it directly to operational plans, emerging threats and responses and specific scenarios.

In the past, we have been able to adapt as a nation to changes in the world. In the 21st century, we are faced with changes that will test America both with respect to how we define ourselves geographically and how we define our freedoms for our citizens. Terrorism tests our borders in both these areas. A 21st century America no longer has fixed physical borders or borders in cyberspace that can be protected in conventional ways. A 21st century America must protect the freedom of its citizens and yet at the same time restrict the freedom of others to prevent terrorist acts.

This report provides a technical view of strategy and policy. It recommends a comprehensive environment in which to create new strategies and policies. It states that technologies, both as threats and responses, will play an ever-increasing role in our society s security. The fabric of our society depends upon both a free and safe America. This will be a formidable task for future policy and strategy formation.

Terrorism, the Future, and U.S. Foreign Policy

Raphael F. Perl

Summary

International terrorism threatens U.S. foreign and domestic security and compromises a broad range of U.S. foreign policy goals. This issue briefly examines emerging international terrorist threats and the U.S. policy response. Available policy options range from diplomacy, international cooperation and constructive engagement to economic sanctions, covert action, physical security enhancement, and military force.

Throughout successive administrations, a key element of stated U.S. policy has remained: no concessions to terrorism. Recent willingness by such groups as the PLO, and IRA to moderate behavior may indicate success of this policy. In this context, current U.S., British, and Israeli policies of engagement with such groups is seen by many as a response to changing circumstances.

Dramatic events, such as the Oklahoma City, World Trade Center, and U.S. embassy bombings in Kenya and Tanzania, as well as the Tokyo subway gas attack, have brought the issue of terrorism to the forefront of American public interest. These specific occurrences raise questions as to whether U.S. policy and organizational mechanisms are adequately focused to combat what may be a new brand of terrorist: one who does not work for any established organization and who is not an agent of any particular state sponsor, yet has access to the most lethal weaponry.

Formal definitions of terrorism do not include terrorist activity for financial profit or terrorists motivated by religious goals. Non-traditional harm such as computer "violence" may not be included either. Such activity may well be on the rise, and policy and organizational mindsets geared to deal with terrorism as politically motivated and violent behavior may limit our ability to combat new and expanding forms of terrorism.

Terrorist access to chemical, biological, or nuclear weaponry raises the specter of mass-casualty attacks. Faced with such prospects, governments are increasingly likely to consider utilizing covert operations to protect their citizenry.

In light of the shifting nature and enhanced intensity of the new terrorist threat, some analysts believe a comprehensive review of U.S. terrorism policy, organizational structure, and preparedness to respond to major terrorist incidents in the United States is desirable. PDD 62, which established a terrorism coordinator at the National Security Council (NSC), may take much of the terrorism decision-making process out of the realm of congressional oversight as NSC members do not generally testify on the Hill.

Radical Islamic fundamentalist groups pose a major terrorist threat to U.S. interests and friendly regimes. Nations facing difficult challenges include Algeria, Bahrain, Egypt, Israel,

Jordan, Pakistan, and to a lesser degree, Russia and Saudi Arabia. One of the seven states on the State Department's terrorism list, Iran, is seen as the most active state sponsor. Iran has been aggressively seeking nuclear weapons technology. Sanctions have not deterred such activity to any meaningful degree. Some see utility in an informal "watch-list" of nations not currently qualifying for inclusion on the terrorism list. See also: CRS Report 98-733, Terrorism: U.S.Response to Bombings in Kenya andTanzania: A New Policy Direction?

Background Analysis

In recent years, terrorism has been primarily viewed as an international and foreign policy issue. Numerous acts of state-sponsored terrorists and of foreign-based groups have given support to this notion. While U.S. policies, citizens, and interests are prime targets for international terrorism in 1999 approximately 52%, up from 40% in 1998, of all terrorist incidents worldwide were committed against U.S. citizens or property according to the U.S. Department of State, and the vast majority of those acts took place on foreign soil. Although terrorism may be internationally motivated, financed, supported or planned, on the receiving end, all terrorism is local. Thus, US public perception of terrorism as primarily an overseas issue may be changing with the bombings of the Trade Center in New York and the Federal Building in Oklahoma City. The predominant method of attack during 1999 was bombing (roughly one-half); the most common targets were business related.

On May 1, 2000, the Department of State released its Patterns of Global Terrorism report (Patterns 1999). In 1999, casualties associated with terrorism worldwide were significantly down from 1998 data. The report indicates that worldwide deaths from terrorist incidents are down roughly threefold from 1998 (from 741 to 233) and the number of wounded was down roughly eightfold from 5,952 to 706. In terms of deaths by region, Asia ranked first; Africa, second; and the Middle East, third. In terms of wounded by region, Asia ranked first, Africa, second, and the Middle East , third as well. In 1998, Africa was highest in both the number of dead and wounded by terrorism; Asia was in second place. In 1999, the number of attacks rose in all regions of the world except the Middle East.

Both timing and target selection by terrorist groups has produced significant political and economic impact on phenomena such as the Middle East peace process and tourism in nations such as Egypt. Some analysts have expressed concern that radical Islamic groups may seek to exploit economic and political instabilities in Saudi Arabia. Other potential target nations of such groups include Algeria, Bahrain, Egypt, India, Jordan, Turkey, and Pakistan. Patterns 1999 suggests that a decline in state sponsorship of terrorism has moved terrorism eastward from Libya, Syria, and Lebanon to South Asia. The result: more U.S. policy focus on Usama bin Laden and the alliance of groups operating out of Afghanistan with the acquiescence of the Taliban. A heavy area of focus remains the ability of terrorists to raise funds through non-state sources, often through charitable contributions, kidnaping, and drug trafficking.

Patterns 1999 cited North Korea, Cuba, and Syria as possible candidates for removal from the list of state sponsors of terrorism (see CRS Report RL30613, North Korea: Terrorism List Removal?). Iran, despite political changes in 1999, is again listed as the most active state sponsor of international terrorism. Iran and Syria were cited for supporting regional terrorist groups, and Lebanon was cited as a key safe haven. Concern was expressed by Russia and Chechnya's neighbors that increased radicalization of Islamist populations would encourage violence and spread instability elsewhere in Russia and beyond. Though not added to the list, Afghanistan and Pakistan were singled out as major sites of terrorist activity.

The bombings of U.S. Embassies in East Africa, of the N.Y. World Trade Center, and of the Jewish cultural center in Buenos Aires may indicate a trend to inflict higher casualties on what are generally less protected civilian targets. It appears that state-sponsored terrorism is decreasing significantly as, in a post-Cold War era, groups find it harder to obtain sponsors and rogue states are less willing to risk exposure to broad based and severe international sanctions. In this environment, access to private sources of funding for terrorist enterprises becomes critical.

International terrorism is recognized as a threat to U.S. foreign and domestic security; it also undermines a broad range of U.S. foreign policy goals. Terrorism erodes international stability, a major foreign and economic policy objective for the United States. Terrorist groups often seek to destabilize or overthrow governments, sometimes democratically elected or friendly governments, and such groups often draw their support from public discontent over the perceived inability of governments to deliver peace, security, and economic prosperity. Efforts by governments to enhance national or regional economic development and stability may become the object of particularly virulent attack. In this regard, and because of their avowed goals to overthrow secular regimes in countries with large Muslim populations, extremist Islamic fundamentalist groups, and Iran s support for such groups, are seen as a major threat to U.S. foreign policy goals and objectives.

Definitions

There is no universally accepted definition of international terrorism. One definition widely used in U.S. government circles, and incorporated into law, defines international terrorism as terrorism involving the citizens or property of more than one country. Terrorism is broadly defined as politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. A terrorist group is defined as a group which practices or which has significant subgroups which practice terrorism (22 U.S.C. 2656f). One potential shortfall of this traditional approach is its focus on groups and group members and exclusion of individual (non-group organized) terrorist activity which has recently risen in frequency and visibility. Another possible weakness of these standard definitions is the criteria of violence in a traditional form. Analysts pointing to "virus" sabotage incidents warn that terrorist s acts could include more sophisticated forms of destruction and extortion such as disabling a national infrastructure by penetrating vital computer software.

Current definitions of terrorism all share one common element: politically motivated behavior. Such definitions do not include violence for financial profit or religious motivation. The rapid growth of transnational criminal organizations and the growing range and scale of such operations could well result in their use of violence to achieve objectives with financial profit as the driving motivation. Thus, although the basic assumption today is that all terrorist acts are politically motivated, some are driven by other factors, and this number may grow in light of expanding international criminal activity and an increasing number of extremist acts carried out in the name of religious and cultural causes. A new approach might focus more on defining terrorist acts, giving less emphasis to the motivation behind the acts.

U.S. Policy Response

Framework

Past administrations have employed a range of options to combat international terrorism, from diplomacy and international cooperation and constructive engagement to economic sanctions, covert action, protective security measures, and military force. The application of sanctions is one of the most frequently used tools of U.S. policymakers. Governments supporting international terrorism (as identified by the Department of State) are prohibited from receiving U.S. economic and military assistance. Export of munitions to such countries is foreclosed, and restrictions are imposed on exports of "dual use" equipment such as aircraft and trucks.

Throughout successive administrations, U.S. policy as publicly stated has remained: no concessions to terrorists, the U.S. government will not pay ransoms, release prisoners, change its policies, nor agree to other acts that might encourage additional terrorism. Practice, however, has not always been so pure. Recent U.S. and Israeli overtures to the PLO, and recent U.S. and British approaches to the IRA clearly appear to reflect some change in approach as such groups begin to moderate their behavior.

Most experts agree that the most effective way to fight terrorism is to gather as much intelligence as possible, disrupt terrorist plans and organizations before they act, and organize multinational cooperation against terrorists and countries that support them. The U.N.'s role in mandating sanctions against Libya for its responsibility in the 1988 Pan Am 103 bombing was significant as the first instance when the world community imposed sanctions against a country in response to its complicity in an act of terrorism. Several factors made the action possible. First, terrorism has touched many more countries in recent years, forcing governments to put aside parochial interests. (Citizens from over 30 countries have reportedly died in Libyan-sponsored bombings.) Second, the end of the Cold War has contributed to increased international cooperation against terrorism. And third, U.S. determination to punish terrorist countries, by military force in some instances, once their complicity was established, was a major factor spurring other countries to join U.N.-sponsored action.

In the past, governments have often preferred to handle terrorism as a national problem without outside interference. Some governments were also wary of getting involved in others battles and possibly attracting additional terrorism in the form of reprisals. Others were reluctant to join in sanctions if their own trade interests might be damaged or they sympathized with the perpetrator s cause. Finally, there is the persistent problem of extraditing terrorists without abandoning the long-held principle of asylum for persons fleeing persecution for legitimate political, or other activity.

Dilemmas

In their desire to combat terrorism in a modern political context, nations often face conflicting goals and courses of action: (1) providing security from terrorist acts, i.e. limiting the freedom of individual terrorists, terrorist groups, and support networks to operate unimpeded in a relatively unregulated environment; versus (2) maximizing individual freedoms, democracy, and human rights. Efforts to combat terrorism are complicated by a global trend towards deregulation, open borders, and expanded commerce. Particularly in democracies such as the United States, the constitutional limits within which policy must operate are often seen to conflict directly with a desire to secure the lives of citizens against terrorist activity more effectively.

Another dilemma for policymakers is the need to identify the perpetrators of particular terrorist acts and those who train, fund, or otherwise support or sponsor them. Moreover, as the international community increasingly demonstrates its ability to unite and apply sanctions against rogue states, states will become less likely to overtly support terrorist groups or engage in state sponsored terrorism.

Today a non-standard brand of terrorist may be emerging: individuals who do not work for any established terrorist organization and who are apparently not agents of any state sponsor. The worldwide threat of such individual or "boutique" terrorism, or that of "spontaneous" terrorist activity such as the bombing of bookstores in the United States after Ayatollah Khomeini's death edict against Salman Rushdie, appears to be on the increase. Thus, one likely profile for the terrorist of the 21st century may well be a private individual not affiliated with any established group. Another profile might be a group-affiliated individual acting independently of the group, but drawing on other similarly minded individuals for support. Because U.S. international counter-terrorism policy framework is sanctions-oriented, and has traditionally sought to pin responsibility on state-sponsors, some policy realignment may be required.

Another problem surfacing in the wake of the number of incidents associated with Islamic fundamentalist groups is how to condemn and combat such terrorist activity, and the extreme and violent ideology of specific radical groups, without appearing to be anti-Islamic in general. A desire to punish a state for supporting international terrorism may also be subject to conflicting foreign policy objectives.

Policy Tools

The U.S. government has employed a wide array of policy tools to combat international terrorism, from diplomacy and international cooperation and constructive engagement to economic sanctions, covert action, protective security measures, and military force.

Diplomacy/Constructive Engagement. Most responses to international terrorism involve use of diplomacy in some form as governments seek cooperation to apply pressure on terrorists. One such initiative was the active U.S. role taken in the March 1996 Sharm al-Sheikh peacemaker/anti-terrorism summit. Another is the ongoing U.S. effort to get Japan and major European nations to join in U.S. trade and economic sanctions against Iran. Some argue that diplomacy holds little hope of success against determined terrorists or the countries that support them. However, diplomatic measures are least likely to widen the conflict and therefore are usually tried first.

In incidents of international terrorism by subnational groups, implementing a policy response of constructive engagement is complicated by the lack of existing channels and mutually accepted rules of conduct between governmental entities and the group in question. In some instances, as was the case with the PLO, legislation may specifically prohibit official contact with a terrorist organization or its members. Increasingly, however, governments appear to be pursuing policies which involve verbal contact with terrorist groups or their representatives.

The media remain powerful forces in confrontations between terrorists and governments. Appealing to, and influencing, public opinion may impact not only the actions of governments but also those of groups engaged in terrorist acts. From the terrorist perspective, media coverage is an important measure of the success of a terrorist act or campaign. And in hostage type incidents, where the media may provide the only independent means a terrorist has of knowing the chain of events set in motion, coverage can complicate rescue efforts. Governments can use the media in an effort to arouse world opinion against the country or group using terrorist tactics. Public diplomacy and the media can be used to mobilize public opinion in other countries to pressure governments to take action against terrorism. An example would be to mobilize the tourist industry to pressure governments into participating in sanctions against a terrorist state. See CRS Report 97-960, Terrorism, The Media, and the Government: Perspectives, Trends, and Options for Policymakers.

Economic Sanctions. In the past, use of economic sanctions was usually predicated upon identification of a nation as an active supporter or sponsor of international terrorism. On August 20, 1998, President Clinton signed an executive order freezing assets owned by Saudi-born Islamic terrorist leader Osama bin Laden, specific associates, and their self-proclaimed Islamic Army Organization, and prohibiting U.S. individuals and firms from doing business with them. Previously, the Clinton Administration had frozen the assets of 12 alleged Middle East terrorist organizations and 18 individuals associated with those organizations. On October 8, 1997, the State Department released a list of 30 foreign terrorist organizations. As of October 1999, the number of organizations on this list stood at 28. The 1996 Antiterrorism and Effective Death Penalty Act makes it a crime to provide support to these organizations, and their members shall be denied entry visas into the United States.

On August 10, 1999, the United States froze the assets of Afghanistan's national airline under sanctions designed to punish the Taliban movement for harboring bin Laden. Apprehension of bin Laden remains a publically announced top priority for the U.S. counter-terrorism community, despite suggestions from some that such policy focus overstates his importance, aids his recruitment efforts, neglects other foreign policy and national security priorities, and diverts resources from other counter-terrorism areas where they are badly needed. In related developments, on July 6, 1999, the United States banned trade with parts of Afghanistan controlled by the Taliban.

Economic sanctions fall into six categories: restrictions on trading, technology transfer, foreign assistance, export credits and guarantees, foreign exchange and capital transactions, and economic access. Sanctions may include a total or partial trade embargo, embargo on financial transactions, suspension of foreign aid, restrictions on aircraft or ship traffic, or abrogation of a friendship, commerce, and navigation treaty. Sanctions usually require the cooperation of other countries to make them effective, and such cooperation is not always forthcoming.

The President has a variety of laws at his disposal, but the broadest in its potential scope is the International Emergency Economic Powers Act. The Act permits imposition of restrictions on economic relations once the President has declared a national emergency because of a threat to the U.S. national security, foreign policy, or economy. While the sanctions authorized must deal directly with the threat responsible for the emergency, the President can regulate imports, exports, and all types of financial transactions, such as the transfer of funds, foreign exchange, credit, and securities, between the United States and the country in question. Specific authority for the Libyan trade embargo is in Section 503 of the International Trade and Security Act of 1985, while Section 505 of the Act authorizes the banning of imports of goods and services from any country supporting terrorism.

Other major laws that can be used against countries sponsoring terrorism are the Export Administration Act, Arms Export Control Act, and foreign assistance legislation. The Export Administration Act (Section 6(j)) allows the President to regulate export of dual use technology and prohibit or curtail the export of critical technology or other technological data. U.S. sales of technology, particularly high technology processes, have been considerable, and sales restrictions or prohibitions are known to have put pressure on states reluctant to control terrorism. Under this Act, exports of various sensitive articles to terrorism-list states are strictly controlled or prohibited because of their support of terrorism. The Arms Export Control Act authorizes the President to restrict the sale of defense articles and restrict or suspend defense services to states fostering terrorism. Foreign assistance authorization and appropriations acts deny foreign aid to countries supporting terrorism and require the U.S. to vote against loans to such countries in the multilateral developments banks. Country specific export control restrictions on munitions list items and dual use equipment apply to Iraq and Iran and are found in the Iraq Sanctions Act (Section 586 of P.L. 101-513). More recently, Executive Orders 12957 and 12959 prohibit U.S. development of Iran's oil industry and U.S. exports to and imports from, Iran, as well as third country reexport of U.S. products to the Islamic Republic. P.L. 104-172, the 1996 Iran Oil Sanction s Act, prohibits U.S. trade with companies that invest more than $40 million in Iran's or Libya's petroleum development, or with companies not complying with U.N. mandated embargoes on sales of oil equipment to Libya. On March 17, 2000, Secretary of State, Albright, announced suspension of a ban on imports of Iranian pistachio nuts, caviar, and carpets a move seen as a gesture to Iranian reformers and their supporters.

P.L. 104-132 prohibits the sale of arms to any country the President certifies is not cooperating fully with U.S. anti-terrorism efforts. The seven terrorist list countries and Afghanistan are currently on this list. Sections 325 and 326 of this law also require that aid be withheld to any country providing lethal military aid to countries on the terrorism list.

On July 6, 1999, President Clinton issued an executive order imposing sanctions against the Taliban and on October 15, 1999, the U.N. Security Council unanimously adopted a resolution imposing limited sanctions against the Taliban. The Council demanded that the Taliban turn over alleged Saudi terrorist suspect Usama bin Laden to a country where he will be effectively brought to justice. Sanctions called for include: (1) denying aircraft landing and takeoffs to and from Taliban controlled territory; and (2) freezing funds and financials resources from Taliban owned or controlled undertakings.

The United States can suspend airline service to and from a nation or deny entry to terrorists and their supporters. In 1978, the United States joined with West Germany, Canada, Britain, France, Italy, and Japan in declaring a willingness to suspend commercial airline service between any of those countries and any country harboring hijackers. Recently, efforts have been made to sanction third-party countries for trading with an already sanctioned country.

Covert Action. Intelligence gathering, infiltration of terrorist groups and military operations involve a variety of clandestine or so called "covert" activities. Much of this activity is of a passive monitoring nature. A more active form of covert activity occurs during events such as a hostage crisis or hijacking when a foreign country may quietly request advice, equipment, or technical support during the conduct of operations, with no public credit to be given to the providing country.

Some nations have periodically gone beyond monitoring or covert support activities and resorted to unconventional methods beyond their territory for the express purpose of neutralizing individual terrorists and/or thwarting preplanned attacks. Examples of activities might run the gamut from intercepting or sabotaging delivery of funding or weapons to a terrorist group, to seizing and transporting a wanted terrorist to stand trial for assassination or murder. Arguably, such activity might be justified as preemptive self-defense under Article 51 of the U.N. charter. On the other hand, it could be argued that such actions violate customary international law. Nevertheless, a July 1989 memorandum by the Department of Justice's Office of Legal Counsel advises that the President has the authority to violate customary international law and can delegate such authority to the Attorney General level, should the national interest so require.

Assassination is specifically prohibited by U.S. Executive Order (most recently, E.O. 12333), but bringing of wanted criminals to the United States for trial is not. There exists an established U.S. legal doctrine that allows an individual's trial to proceed regardless of whether theperson is forcefully abducted from another country, or from international waters or airspace. For example, Fawaz Yunis, a Lebanese who participated in the 1985 hijacking of a Jordanian airliner, with two Americans among its 70 passengers, was lured aboard a yacht in international waters off the coast of Cyprus in 1987 by federal agents, flown to the United States for trial, and convicted.

Experts warn that bringing persons residing abroad to U.S. justice by means other than extradition or mutual agreement with the host country, i.e., by abduction and their surreptitious transportation, can vastly complicate U.S. foreign relations, perhaps jeopardizing interests far more important than "justice," deterrence, and the prosecution of a single individual. For example, the abduction of a Mexican national in 1990 to stand trial in Los Angeles on charges relating to torture and death of a DEA agent led to vehement protests from the government of Mexico, a government subsequently plagued with evidence of high level drug related corruption. Subsequently, in November 1994, the two countries signed a treaty to Prohibit Transborder Abductions. Notwithstanding the unpopularity of such abductions in nations that fail to apprehend and prosecute those accused, the "rendering" of such wanted criminals to U.S. courts is permitted under limited circumstances by a January 1993 Presidential Decision Directive issued under the Bush Administration, and reaffirmed by President Clinton. Such conduct, however, raises prospects of other nations using similar tactics against U.S. citizens.

Although conventional explosives specifically car bombs appear to be the terrorism weapon of choice, the world is increasingly moving into an era in which terrorists may gain access to nuclear, chemical, or biological weaponry. Faced with the potential of more frequent incidents and higher conventional casualty levels, or a nuclear or biological holocaust, nations may be more prone to consider covert operations designed to neutralize such threats.

Rewards for Information Program. Money is a powerful motivator. Rewards for information have been instrumental in Italy in destroying the Red Brigades and in Colombia in apprehending drug cartel leaders. A State Department program is in place, supplemented by the aviation industry, offering rewards of up to $4 million to anyone providing information that would prevent or resolve an act of international terrorism against U.S. citizens or U.S. property, or that leads to the arrest or conviction of terrorist criminals involved in such acts. This program was at least partly responsible for the arrest of the Unabomber, of Ramzi Ahmed Yousef, the man accused of masterminding the World Trade Center bombing, and of the CIA personnel shooter, Mir Amal Kansi. The program was established by the 1984 Act to Combat International Terrorism (P.L. 98-533), and is administered by State's Diplomatic Security Service. Rewards over $250,000 must be approved by the Secretary of State. The program can pay to relocate informants and immediate family who fear for their safety. The 1994 "crime bill" (P.L. 103-322) helps relocate aliens and immediate family members in the U.S. who are reward recipients. Expanded participation by the private sector in funding and publicizing such reward programs has been suggested by some observers.

Extradition/Law Enforcement Cooperation. International cooperation in such areas as law enforcement, customs control, and intelligence activities is an important tool in combating international terrorism. One critical law enforcement tool in combating international terrorism is extradition of terrorists. International extradition traditionally has been subject to several limitations, including the refusal to extradite for political or extraterritorial offenses and the refusal of some countries to extradite their nationals. The United States has been encouraging the negotiation of treaties with fewer limitations, in part as a means of facilitating the transfer of wanted terrorists. Because much terrorism involves politically motivated violence, the Department of State has recently sought to curtail the availability of the political offense exception, found in many extradition treaties, to avoid extradition.

Military Force. Although not without difficulties, military force, particularly when wielded by a superpower such as the United States, can carry substantial clout. Proponents of selective use of military force usually emphasize the military's unique skills and specialized equipment. The April 1986 decision to bomb Libya for its alleged role in the bombing of a German discotheque exemplifies use military force. Other examples are: (1) the 1993 bombing of Iraq's military intelligence headquarters by U.S. forces in response to Iraqi efforts to assassinate former president George Bush during a visit to Kuwait, and (2) the August 1998 missile attacks against bases in Afghanistan and a chemical production facility in Sudan.

Concerns about a terrorist threat prompted an extensive buildup of the military's counterterrorist organization. A special unit known as "Delta Force" at Fort Bragg, NC, has been organized to perform anti-terrorist operations when needed. Details about the unit are secret, but estimates are that it has about 800 assigned personnel.

Use of military force presupposes the ability to identify a terrorist group or sponsor and its location, knowledge often unavailable to law enforcement officials. Risks of military force include: (1) military casualties or captives; (2) foreign civilian casualties; (3) retaliation and escalation by terrorist groups; (4) holding the wrong parties responsible; (5) sympathy for the "bullied" victim; and (6) perception that the U.S. ignores rules of international law.

P.L. 104-264 includes a sense of the Senate statement that if evidence suggests "beyond a clear and reasonable doubt" that an act of hostility against any U.S. citizen was a terrorist act sponsored, organized, condoned or directed by any nation, then a state of war should be considered to exist between the United States and that nation.

International Conventions. To date, the United States has joined with the world community in developing all of the major anti-terrorism conventions. These conventions impose on their signatories an obligation either to prosecute offenders or extradite them to permit prosecution for a host of terrorism-related crimes including hijacking vessels and aircraft, taking hostages, and harming diplomats. An important new convention not yet in force is the Convention for the Marking of Plastic Explosives. Implementing legislation is in P.L. 104-132. On December 8, 1999, the U.N. General Assembly adopted the Anti-Terrorism Financing Convention that grew out of G-8 nation endeavors to combat terrorist financing.

Potential Tools

An International Court for Terrorism. Each year bills are introduced urging that an international court be established, perhaps under the U.N., to sit in permanent session to adjudicate cases against persons accused of international terrorist crimes. The court would have broad powers to sentence and punish anyone convicted of such crimes. Critics point out many administrative and procedural problems associated with establishing such a court and making it work, including jurisdictional and enforcement issues. An International Court of Justice in the Hague exists, but it deals with disputes between states, and lacks compulsory jurisdiction and enforcement powers.

Media Self-Restraint. For some, the term "media self-restraint" is an oxymoron; the sensational scoop is the golden fleece and dull copy is to be avoided. While some of the media struggle to maintain objectivity, they are occasionally manipulated into the role of mediator and often that of publicist of terrorist goals. Though not an international incident, the publication of the Unabomber's "manifesto" illustrated this. Notably, there have been attempts by the media to impose its own rules when covering terrorist incidents. Standards established by the Chicago Sun-Times and Daily News include paraphrasing terrorist demands to avoid unbridled propaganda; banning participation of reporters in negotiations with terrorists; coordinating coverage through supervising editors who are in contact with police authorities; providing thoughtful, restrained, and credible coverage of stories; and allowing only senior supervisory editors to determine what, if any, information should be withheld or deferred. Such standards are far from uniformly accepted. In an intensely competitive profession consisting of a multinational worldwide press corps, someone is likely to break the story. See CRS Report 97-960, Terrorism, the Media, and the Government: Perspectives, Trends and Options for Policymakers.

Policy Reform

On June 5, 2000, the National Commission on Terrorism (NTC), a congressionally mandated bi-partisan body, issued its report which included a blueprint for U.S. counterterrorism policy with both policy and legislative recommendations.

The NTC report is likely to stimulate strong congressional interest in counterterrorism policy when the 107th Congress convenes in January 2001. Likely areas of focus are (1) a more proactive counterterrorism policy; (2) a stronger state sanctions policy; and (3) a more cohesive/better coordinated U.S. federal counterterrorism policy. (See CRS Report RS20598, National Commission on Terrorism Report: Background and Issues for Congress.)

U.S. Organization and Program Response

The chain of command on anti-terrorism planning runs from the President through the National Security Council, a representative of which chairs a senior interagency Terrorism Security Group (TSG). The State Department is designated the lead agency for countering terrorism overseas; the Justice Department's Federal Bureau of Investigation (FBI) is the lead agency for domestic terrorism; and the Federal Aviation Administration is the lead for hijackings when a plane's doors are closed. These roles were reaffirmed by Presidential Decision Directive (PDD) No. 39 in June 1995. PDD 62 (Protection Against Unconventional Threats) and PDD 63 (Critical Infrastructure Protection) of May 22, 1998: (1) established within the NSC a National Coordinator for Security, Infrastructure Protection, and Counterterrorism who also provides "advice" regarding the counterterrorism budget; (2) established within the NSC two Senior Directors who report to the National Coordinator one for infrastructure protection and one for counterterrorism; (3) established a new inter-agency working group primarily focused on domestic preparedness for WMD incidents; and (4) laid out the architecture for critical infrastructure protection. Intelligence information among the various agencies is coordinated by an Intelligence Committee, and chaired by a representative of the CIA. An important policy question is whether current organizational structure brings excessive focus on state-sponsored actions at the expense of attention on so-called "gray area" terrorist activity (i.e., terrorist activity not clearly linked to any perpetrator, group, or supporting/sponsoring nation). In light of recent trends in terrorist activity, some suggest that an independent comprehensive review of counter-terrorism policy, organizational structure, and preparedness to respond to major terrorist incidents in the United States is warranted. Whether PDD 62, by establishing a national terrorism coordinator at the NSC, takes too much of the terrorism decisionmaking process out of the realm of congressional oversight is another issue as NSC members generally do not testify before Congress.

A number of Administration programs focus specifically on combating international terrorism. They include the Department of State's: (1) Anti-Terrorism Assistance Program (ATA); (2) Counter-Terrorism Research and Development Program; and (3) Diplomatic Security Program. The DOD Authorization Act (Title XIV) for FY1997 (P.L. 104-201) seeks to ensure DOD assistance to federal, state, and local officials in responding to biological, chemical, and nuclear emergencies.

On January 22, 1999, President Clinton announced a $10 billion initiative to address terrorism. Included were $1.4 billion to protect against chemical and biological terrorism and $1.46 billion to protect critical systems from cyber and other attacks.

Anti-Terrorism Assistance Program

The State Department's anti-terrorism assistance program provides training and equipment to foreign countries to help them improve their anti-terrorism capabilities. More than 20,000 individuals from 100 countries have received training since the program's inception in 1983 in such skills as crisis management, VIP protection, airport security management, and bomb detection and deactivation. The Administration's FY1998 $18 million request for this program was fully funded at $19 million; the FY1999 request totaled $21 million and was funded at $41 million (which included $20 million from a FY1999 emergency security supplemental appropriations), and the FY2000 request was $23 million.

Counter-Terrorism Research and Development Program

The State Department's Counter-Terrorism Research and Development Program, which is jointly funded by the Departments of State and Defense, constitutes a response to combat the threat posed by increasingly sophisticated equipment and explosives available to terrorist groups. Recent projects include detectors for nuclear materials, decontaminates for chemical and biological weapons, law enforcement and intelligence database software and surveillance technology. The State Department's FY1997- FY2000 budget requests for these programs totaled $1.8 million. DOD's FY2000 request totaled $52.2 with a $54.8 million request projected for FY2001.

Diplomatic Security Program

The Diplomatic Security Program of the State Department is designed to protect U.S. personnel, information, and facilities abroad. Providing security guards and counterintelligence awareness are important elements of the program. Detection and investigation of passport and visa fraud is another component of the program.

The Administration's FY2000 request for the Diplomatic Security Program is $226.514 million. One component of the broader program provides protection of international organizations, foreign missions and officials under the Foreign Missions Act of 1982. Security enhancement for U.S. embassies is funded through the "Acquisition and Maintenance of Buildings Abroad" account. The FY1999 request was $640.8 million with $1,030.6 million appropriated.

The State Department's FY2000 request to Congress includes $568 million for embassy security (see CRS Report 98-771, Embassy Security: Background, Funding, and the FY2000 Budget). The Administration included in its State Department request an advance appropriation of $3 billion for FY2001-FY2005. Beginning with a FY2001 baseline of $300 million, the Administration will allocate these funds in additional $150 million increments each year ending with $900 million for FY2005.

Options for Program Enhancement

Numerous options have been proposed to improve the effectiveness of programs designed to combat terrorism. Some notable areas cited for improvement include contingency planning; explosives detection; joint or multinational research, operational and training programs/exercises; nuclear materials safeguarding; and disaster consequence management. Some have suggested that U.S. public diplomacy/media programs could be broadened to support anti-terrorism policy objectives. Cyber security remains an important area for program enhancement. On January 9, 2000, the Administration released a comprehensive plan to combat cyber-terrorism including

$2 billion in proposed spending next year to make the nation's computer systems less vulnerable to attack. Plan elements include: (1) enhanced funding for research and development; (2) creation of a ROTC-type corps of information specialists; and (3) creation of a national institute charged with forging a research partnership with the private sector.

State-Supported Terrorism

The Secretary of State maintains a list of countries that have "repeatedly provided support for acts of international terrorism." Data supporting this list are drawn from the intelligence community. Listed countries are subject to severe U.S. export controls, particularly of dual use technology, and selling them military equipment is prohibited. Providing foreign aid under the Foreign Assistance Act is also prohibited. Section 6(j) of the 1979 Export Administration Act stipulates that a validated license shall be required for export of controlled items and technology to any country on the list, and that the Secretaries of Commerce and State must notify the House Committee on Foreign Affairs, and both the Senate Committees on Banking, Housing, and Urban Affairs, and Foreign Relations, at least 30 days before issuing any validated license required by this Act. In addition, Section 509(a) of the 1986 omnibus anti-terrorism act (P.L. 99-399) bars export of munitions list items to countries on the terrorism list. Indirect state sponsorship or sponsorship by proxy is addressed in a second State Department terrorist list (required by P.L. 104-132) which is distinct from the list of state sponsors generally referred to as the "list" prohibits the sale of arms to nations not fully cooperating with U.S. anti-terrorism efforts. Strong language critical of Greece in Patterns 1999 prompts some to question whether Greece should be included in the latter category of nations. The current list of countries not fully cooperating includes the seven state supporters plus Afghanistan. P.L. 104-132 also requires the withholding of foreign assistance to nations providing lethal military aid to countries on the list of state sponsors.

Adding and Removing Countries on the List

In late January each year, under the provisions of Section 6(j) of the Export Administration Act of 1979, as amended, the Secretary of Commerce in consultation with the Secretary of State provides Congress with a list of countries supporting terrorism. Compilation of the list is the result of an ongoing process. Throughout the year the Department of State gathers data on terrorist activity worldwide, and then beginning about November, the list is formally reviewed. Each new determination under Section 6(j) of the Act must also be published in the Federal Register. (For removal criteria see CRS Report RL30613, North Korea: Terrorism List Removal?)

Paragraph 6(j)(4) of the Export Administration Act prohibits removing a country from the list unless the President first submits a report to the House Committee on Foreign Affairs, and the Senate Committees on Banking, Housing, and Urban Affairs, and Foreign Relations. When a government comes to power (i.e., a government different from that in power at the time of the last determination), the President s report, submitted before the proposed rescission would take effect, must certify that: (1) there has been a fundamental change in the leadership and policies of the government of the country concerned (this means an actual change of government as a result of an election, coup, or some other means); (2) the new government is not supporting acts of international terrorism; and (3) the new government has provided assurances that it will not support acts of international terrorism in the future. When the same government is in power, the

President's report   **submitted at least 45 days before the proposed rescission would take effect**   must justify the rescission and certify that: (1) the government concerned has not provided support for international terrorism during the preceding 6-month period; and (2) the government concerned has provided assurances that it will not support acts of international terrorism in the future. Congress can let the President's action take effect, or pass legislation to block it, the latter most likely over the President s veto. To date, Congress has passed no such legislation or resolution, although Syria would be the likely target of such endeavors, should the Administration prematurely seek its removal from the terrorism list. Patterns 1999 notes that "if a state sponsor meets the criteria from being dropped from the terrorism list, it will be removed notwithstanding other differences we may have with a country's other policies and actions."

Countries on the List

Currently seven countries are on the "terrorism list": Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. [For further information on states sponsoring international terrorism, see Patterns of Global Terrorism (Patterns 1999), Department of State, April 2000.] Of the seven, five are Middle Eastern nations with predominantly Muslim populations. (See CRS Report 98-722, Terrorism: Middle Eastern Groups and State Sponsors). Of these, Iran and Iraq could currently be characterized on one extreme as active supporters of terrorism: nations that use terrorism as an instrument of policy or warfare beyond their borders. Iran, Iraq, and Libya are major oil producers, holding 17% of the world's remaining oil and producing, in 1994, 5.5% of the world's oil supply, 31% of Europe's (OECD) oil consumption, and 9% of Japan's. Such dependence on oil complicates universal support for sanctions against these nations.

On the other extreme one might place countries such as Cuba or North Korea, which at the height of the Cold War were more active, but in recent years have seemed to settle for a more passive role of granting ongoing safe haven to previously admitted individual terrorists. Closer to the middle of an active/passive spectrum is Libya, which grants safe haven to wanted terrorists. Syria, though not formally detected in an active role since 1986, reportedly uses groups in Syria and Lebanon to project power into Israel and allows groups to train in territory under its control, placing it somewhere in the middle to active end of the spectrum. And Sudan, which allows sites for training, remains an enigma. Although Sudan has been considered primarily a passive supporter, charges have been made that Sudan was actively involved in a 1995 attempt to assassinate Egyptian President Hosni Mubarak.

A complex challenge facing those charged with compiling and maintaining the list is the degree to which diminution of hard evidence of a government's active involvement indicates a real change in behavior, particularly when a past history of active support or use of terrorism as an instrument of foreign policy has been well established. Removing a country from the list is likely to result in some level of confrontation with Congress, so the bureaucratically easier solution is to maintain the status quo, or add to the list, but not to delete from it.

Iran. In a change from Patterns 1998, Patterns 1999 names Iran as the most active state sponsor of terrorism despite acknowledged political changes in Iran during 1999. Iran continues to be deeply involved in the planning and execution of terrorist acts by its own agents and surrogate groups. It provides ongoing direction, safe haven, funding, training, weapons and other support to a variety of radical Islamic terrorist groups including Hizballah in Lebanon, as well as Hammas and Palestinian Islamic Jihad (PIJ) to undermine the Middle East peace process. There are press reports that Iran is building a terrorist infrastructure in the region by providing political indoctrination, military training, and financial help to dissident Shia groups in neighboring countries, including Kuwait, Bahrain, and Saudi Arabia. Iran has reportedly concentrated efforts to make Sudan a center for terrorist training and activities and reportedly continues to conduct assassinations of writers and political dissidents beyond its borders. Iran was placed on the terrorism list in January of 1984. President Clinton has halted U.S. trade with Iran and barred U.S. companies from any involvement in the Iranian oil sector. The threat perceived from Iran as a leading supporter of terrorism is substantially raised by reports that Iran is acquiring nuclear technology and seeking nuclear weapons technology.

Iraq. On September 13, 1990, Iraq was placed once again on the terrorism list, after having been removed in 1982. Iraq's ability to instigate terror has been curbed by U.S. and U.N. sanctions which were imposed after the Kuwait invasion. Nevertheless, Patterns 1999 indicates that Saddam Hussein's regime continues to murder dissidents and provide a safe haven for a variety of Palestinian rejectionist groups. There are numerous claims that the Iraqi intelligence is behind killings and at least one planned bombing during 1999. Iraq also provides active assistance to the MEK, a terrorist group opposed to the Teheran regime. In the past, Iraq has temporarily expelled terrorists, only to invite them back later.

Libya. Libya has a long history of involvement in international terrorism. Libya was placed on the terrorism list when it was started in December 1979, and approximately $1 billion in bank deposits belonging to Libya are frozen by the United States. Libyan terrorism has been sharply reduced after imposition of U.N. sanctions in the wake of Libyan involvement in the bombings of Pan Am flight 103 and in the 1989 bombing of French UTA flight 772 that killed 170 persons, including seven Americans. Evidence suggests Libya has not abandoned its support for international terrorism as an instrument of foreign policy, and it still refuses to hand over some accused of terrorist acts. Throughout 1998, Libya continued to support groups opposed to the Mid-East peace process that engage in violence. Nevertheless, the response of the international community and U.S. Congress (P.L. 104-172) seems to have been relatively effective in restraining the level of Libya's outlaw behavior and may provide one model for future international action. There is no evidence of Libyan involvement in recent acts of international terrorism. In April 2000, Libya took what Patterns 1999 notes as "an important step by surrendering ... two Libyans accused of bombing Pan Am flight 103 ... in 1988."

Syria. Syria was placed on the first terrorism list in December 1979. It is generally believed within the western community that Syria has a long history of using terrorists to advance its own interests. The United States has said that it has no evidence of Syrian government direct involvement in terrorism since 1986. Informed sources suggest, however, that the Syrian government remains active, hiding behind the sophisticated operational level of their intelligence services and their ability to mask such involvement. Many major terrorist groups are known to maintain an active presence (including training camps and operational headquarters) in Syria or in Syrian-controlled Lebanon and Syria has allowed Iran to supply Hizballah with weaponry via Damascus. Providing such support, free movement, and safe haven has caused prominent Members of Congress to contend that Syria should remain on the terrorism list, and Administration spokespersons have firmly maintained in testimony before Congress that until this problem is resolved, Syria will remain on the list. In contrast, the Administration has made it clear to Syria that it will consider removing Syria from the list should a peace treaty with Israel be signed. Some observers argue that Syria should continue to be subject to U.S. sanctions because of involvement in drug trafficking by some of its ruling elites and their alleged involvement in counterfeiting of U.S. currency.

Sudan. Sudan was added to the terrorism list in August 1993. Sudan continues to harbor members of some of the world's most violent organizations and according to Patterns 1999 continues to serve as a refuge, nexus, and training hub for a number of terrorist organizations including Hizballah, Hamas, and bin Laden s al-Qaida organization. Egypt and Ethiopia have charged the Sudanese government with involvement in a failed assassination attempt against President Hosni Mubarak while in Ethiopia in June 1995. On September 11, 1995, the Organization for African Unity (OAU), in an unprecedented action criticizing a member, passed a resolution calling on Sudan to extradite three suspects charged in the assassination attempt to Ethiopia. The U.N. Security Council has also demanded extradition of the three suspects. Sudan continues to permit its territory to be used by Iran to transport weapons to Islamic extremist groups and as a meeting place for Iranian-backed terrorist groups.

Cuba. Fidel Castro's government has a long history of providing arms and training to terrorist organizations. A cold war carryover, Cuba was added to the 1982 U.S. list of countries supporting international terrorism based on its support for the M-19 guerrilla organization in Columbia. Patterns 1999 does not cite evidence that Cuban officials were directly involved in sponsoring an act of terrorism in 1999, but notes that Havana remains a safe haven to several international terrorists. The report noted that Cuba no longer actively supports armed struggles in Latin America or elsewhere. Nevertheless, Havana continues to maintain close ties to other state sponsors of terrorism. The Castro regime also reportedly maintains close ties with leftist insurgent groups in Latin America.

North Korea. North Korea was added to the "official" list of countries supporting terrorism because of its implication in the bombing of a South Korean airliner on November 29, 1987, which killed 115 persons. According to the State Department, North Korea is not conclusively linked to any terrorist acts since 1987. A North Korean spokesman in 1993 condemned all forms of terrorism, and said his country resolutely opposed the encouragement and support of terrorism. A similar statement was made in November 1995. Nevertheless, North Korea continues to provide political sanctuary to members of a group that hijacked a Japan Airlines flight in 1970 and may be linked to the murder of a South Korean diplomat in Vladivostoc in 1996. Patterns 1999 notes that North Korea has made "some positive statements condemning terrorism in all its forms" and has stressed that actions triggering removal from the list "are consistent with its stated policies."

An Informal Watchlist?

Some suggest that there is utility in drawing to Congress attention countries that do not currently qualify for inclusion in the terrorism list but where added scrutiny may be warranted. Such a list would be similar to the Attorney General's National Security Threat List that includes sponsors of international terrorism, the activities of which warrant monitoring by the FBI within the United States. Although informal, it would be controversial and speculative. However, it would reflect legitimate concerns of those in the intelligence and policy community and might serve as an informal warning mechanism to the countries that their activities are being scrutinized. For example, the State Department warned Pakistan in January 1993 that it was under "active continuing review" to determine whether it should be placed on the terrorism list. When the list came out in April 1993, Pakistan was not on it. (See CRS Issue Brief IB 94041, Pakistan-U.S. Relations) Sudan was also warned that it was being subject to special review prior to its being placed on the terrorism list in August 1993.

Currently, some informally discussed candidates for such a list include (1) **Afghanistan**—Patterns 2000 characterizes as "the primary safe haven for terrorist." Concerns are that Islamic fundamentalist terrorists linked to numerous international plots continue to train and operate out of the country and/or enter or exit with impunity, and more specifically that the Taliban continues to offer sanctuary to Osama bin Laden and his associated terror networks; (2) **Pakistan** —Patterns 2000 notes that Pakistan has tolerated terrorists living and moving freely within its territory, supported groups that engage in violence in Kashmir, and provided indirect support for terrorists in Afghanistan; (3) **Yugoslavia**—concerns remain over potential use of terrorism in reaction to NATO military operations. Another concern is that militant Iranian elements remaining in terrirtory of former Yugoslavia may resort to terrorist violence against European nations and the United States; (4) **Lebanon**—growing concern exists over terrorist groups operating with impunity from there, often under Syrian protection; (5) **Greece**— Patterns 2000 describes as "one of the weakest links in Europe's efforts against terrorism" and where the absence of strong government measures allows terrorists "to act with virtual impunity"; and (6) **Yemen**—a growing safe haven for international terrorist groups where a growing kidnaping industry flourishes. Patterns 2000 also reflects a growing concern in policy circles that **Chechnya** may increasingly become a magnet and rallying center for Islamic radicals and notes that concern exists that "increased radicalization of Islamist populations connected to the **Chechnya** conflict would encourage violence and spread instability elsewhere in Russia and beyond."

National Commission on Terrorism Report: Background and Issues for Congress

Raphael F. Perl

Summary

On June 5, 2000, the National Commission on Terrorism (NTC), a congressionally mandated bi-partisan body, issued a report providing a blueprint for U.S. counter-terrorism policy with both policy and legislative recommendations. The report could be significant in shaping the direction of U.S. policy and the debate in Congress. It generally argues for a more aggressive U.S. strategy in combating terrorism. Critics, however, argue that NTC conclusions and recommendations ignore competing U.S. goals and interests; i.e. that a proactive strategy might lead to the curbing of individual rights and liberties, damage important commercial interests, and widen disagreements between the U.S. and its allies over using the "stick" as opposed to the "carrot" approach in dealing with states that actively support or countenance terrorism.

The NTC report is likely to stimulate strong congressional interest in counterterrorism policy when the 107th Congress convenes in January 2001. Likely areas of focus are: (1) a more proactive counterterrorism policy; (2) a stronger state sanctions policy; and (3) a more cohesive/better coordinated U.S. federal counterterrorism response. This report will be updated as events require.

Background

Combating terrorism has emerged as one of the most important U.S. foreign policy and national security priorities. The number of terrorist groups is reportedly growing, and the technology to inflict mass casualties is becoming more readily available. The United States and other cooperating nations confront four major tasks, namely: (1) deterring/identifying terrorists and their sponsors/supporters; (2) weakening terrorist financial and other infrastructures; (3) hardening potential targets; and (4) containing damage in the aftermath of terrorist incidents.

Six months ago, in response to what is seen as a growing threat, the U.S. Congress created the ten-person, bi-partisan National Commission on Terrorism to evaluate U.S. laws, policies, and practices for preventing and punishing terrorism aimed at U.S. citizens [P.L. 105-277]. The resulting report, Countering the Changing Threat of International Terrorism, was issued on June 5, 2000. It calls on the U.S. government to prepare more actively to prevent and deal with a future mass casualty, catastrophic terrorist attack.

The report advocates: (1) using full, and what can be characterized as proactive, intelligence and law enforcement authority to collect intelligence regarding terrorist plans and methods; (2)

targeting firmly, and with sanctions, all states that support terrorists; (3) disrupting non-governmental sources of terrorist support, especially financial and logistical; (4) enhancing planning and preparation to respond to terrorist attacks involving biological, chemical, radiological or nuclear materials; and (5) creating stronger mechanisms to ensure that funding for individual agency counterterrorism programs reflects priorities integrated into a comprehensive national counterterrorism plan subject to congressional oversight.

The report suggests that the United States is drifting away from a strong policy of combating state support of international terrorism and is generally too passive and not proactive enough in combating a threat that is becoming more deadly, diffuse, and difficult to detect. Implicit in the report is the suggestion that the United States, by drifting away from a strong policy to combat state support of international terrorism, may well be encouraging more terrorism. In citing incidences of such a drift in policy, the report suggests that there is a softening of U.S. positions on Iran and Syria, and points to a perceived U.S. weakness in not aggressively confronting Pakistan's support for terrorist groups. It also notes U.S. failure to use sanctions, or the threat thereof, in response to Greece's inactivity/reluctance to investigate and prosecute terrorist activity inaction by Greece which is portrayed as tantamount to complicity. While recognizing the growing danger posed by lone-wolf terrorists and loosely affiliated private transnational groups, the report intimates that U.S. policy may be too heavily focused on Usama Bin Laden.

Highlights of the Report

Areas addressed in the report's recommendations include the following:

- Expanding sanctions on state sponsors/uncooperative nations

Greece and Pakistan. The report notes that "Greece has been disturbingly passive in response to terrorist activities." It comments that since 1975 there have been 146 terrorist attacks against Americans or American interests in Greece with only one case being solved and no meaningful investigation into the others. The report cites examples of past Pakistani anti-terrorism cooperation but stresses that "Pakistan provides safehaven, transit, and moral, political, and diplomatic support to several groups engaged in terrorism" [in Kashmir].

The NTC recommends that the President consider imposing sanctions against Greece and Pakistan under provisions of U.S. law [P.L.104-132] that limit arms sales to countries not "fully cooperating" with the U.S. on anti-terrorism efforts. Enactment of legislation, making countries which have been designated as not "fully cooperating" with U.S. counterterrorism efforts, ineligible for the U.S. visa waiver program is also called for. In general, the Commission recommends expanding the broad use of sanctions to include not just state sponsors, but nations not fully cooperating. Currently, U.S. law also requires the withholding of foreign assistance to nations providing lethal military assistance to nations on the U.S. list of state sponsors of terrorism a little-known provision of P.L.104-132, but one that the Administration has used to help persuade some countries to not provide arms to terrorist list states.

Iran. The report expresses concern that U.S. efforts to signal support for political reform in Iran could be misinterpreted in Iran or by U.S. allies as a weakening of resolve on counterterrorism. The report calls for the President to make no further concessions to Iran and to keep Iran on the terrorism sponsors list until it ceases to support terrorism and cooperates fully in the investigation of the June, 1996 Khobar Towers bombing which resulted in the death of U.S. servicemen in Saudi Arabia. It also calls upon the President to actively seek support from U.S. allies to compel Iranian cooperation in the Khobar towers investigation.

Syria. The report recommends that the President make it clear that Syria will remain on the state sponsors list until it shuts down terrorist training camps in Syria and the Bekaa valley and prohibits resupply of terrorist groups through Syrian controlled territory.

Afghanistan. The report notes that the United States has not designated Afghanistan as a state sponsor of terrorism because it does not recognize the Taliban regime. Nevertheless, it recommends designating Afghanistan as state sponsor and imposing sanctions against the Kabul regime.

- Role of the Armed Forces

Under extraordinary circumstances when a catastrophic event is beyond the capabilities of local, state, and other federal agencies, or is directly related to an armed conflict overseas, the report suggests that the President may want to consider designating the Department of Defense (DoD) as the lead federal agency for the government s response in the event of a catastrophic terrorist attack on U.S. soil. The report calls for detailed contingency plans for the Defense Department's role, which could include transfer of command authority to the Pentagon, in the event of a catastrophic event where the command and control, logistical, communications, and specialized ability of the military to respond to chemical/biological/radiological incidents would be required. The Commission believes that advance planning is the best way to prevent curtailment of individual liberties in a weapons of mass destruction scenario.

- Enhancing foreign student visa data retrieval capability

Critics of current Immigration and Naturalization Service (INS) student visa status tracking mechanisms often refer to them as being in the "stone age." In a move which has been characterized as an effort to "substitute computers for shoeboxes," the report recommends expanding an existing computerized pilot program designed to facilitate data retrieval capability to more efficiently monitor the immigration/visa status of students from abroad. This would facilitate access to whereabouts of students from terrorist-list countries and could "flag" a student from such a country who suddenly changes majors from a field such as art to biochemistry or nuclear physics. The report notes that one of the convicted terrorists involved in the World Trade Center bombing entered the U.S. on a student visa, dropped out, and remained illegally thereafter.

- Full use of law enforcement and intelligence authority

The report recommends that existing CIA guidelines restricting recruitment of unsavory (criminal) sources not apply to recruiting counterterrorism sources. Also recommended is that the FBI guidelines governing criteria for investigating suspected terrorists or groups be clarified to permit full use of legal authorities including the authority to conduct electronic surveillance.

- Expulsion of suspected terrorists

Expulsion of suspected terrorists can be a touchy civil liberties issue. In a move designed to minimize what some see as past governmental abuse in expulsion cases handled by INS procedures, the report recommends use of the Alien Terrorist Removal Court (ATRC; created by Congress in 1996 by section 401 of P.L. 104-132, but heretofore unused) to expel terrorists from the United States in instances where criminal prosecution is not possible. This process contains safeguards designed to protect national security and classified evidence (sources and methods), but also accords the accused the right to challenge such evidence.

- National terrorism response exercises

The report recommends that senior federal government officials involved in responding to a catastrophic terrorist threat or incident be required to participate in national response exercises every year to test capabilities and coordination.

- Cyberterrorism/cybercrime

The report calls on the Secretary of State to take the lead in developing an international convention aimed at harmonizing national laws, sharing information, providing early warning, and establishing accepted procedures for conducting international investigations of cybercrime.

- Counterterrorism budget process

The report recommends that the senior National Security Council (NSC) official in charge of coordinating overall U.S. counterterrorism efforts be given a stronger hand in the budget process and that Congress develop a mechanism for comprehensive review of this process and consolidate the process in fewer committees.

Issues for Congress

Protecting civil liberties, while effectively combating terrorism, remains a strong area of concern in Congress. A number of the Commission's recommendations have drawn sharp criticism from civil libertarian and Arab-American groups. This is especially true of those recommendations which relate to: (1) enhancing intelligence gathering; (2) modernizing retrieval capability of databases which monitor the visa status of foreign students; (3) expulsion of suspected terrorists; and (4) contingency planning for an active military role (including a possible lead role) in the event of a catastrophic terrorist attack on U.S. soil. In addition, it is interesting to note that although the Commission's report addresses an impressive array of counterterrorism issues, the list of issues examined is less than exhaustive, leaving a few complex, unresolved, and potentially "prickly" issues unaddressed. These issues would seem to warrant additional congressional attention.

- Civil Liberties Concerns

In democracies such as the United States, the constitutional limits within which policy must operate are sometimes seen to conflict with a desire to more effectively secure the lives of citizens against terrorist activity. Combating terrorism requires government activity designed to gather information on, and restrict the activities of, individual terrorists and groups seeking to engage in direct or indirect terrorist activity. The greater the magnitude of any such acts, the greater the pressure on societal institutions to provide security for their citizens. A challenge facing the policy community is how, in a growing age of globalization, deregulation, democracy and individual freedom, to institute regulatory and monitoring mechanisms which help deter, identify, and track terrorists and generally hinder their operations. Implicit in the reasoning of the Commission's report is that combating terrorism, particularly in the wake of a mass casualty catastrophic incident, may require restrictions on individual liberties. The assumption is that carefully planned and measured restrictions in advance of a catastrophic incident, coupled with well thought out contingency planning for a constructive military role in the aftermath of an incident, constitute an effective way of preserving, and not diminishing, individual liberties and democratic freedoms and institutions.

- Unresolved Issues

The report is noteworthy for what it does not address as well as for what it addresses. Areas not covered in the Commission's report, but dealt with by other panels or expert advisory groups, include: (1) U.S. embassy security (1999 Overseas Advisory Panel Report); (2) security of U.S. military installations overseas (1996 Downing Commission Khobar Towers Report); and (3) weapons of mass destruction (WMD) disaster consequence management (1999 Gilmore Commission Report).

Issues within the purview of the Commission's mandate, but not addressed in its report or in the reports cited above include:

(1) Who should be in charge of U.S. counterterrorism policy, and what are the best organizational mechanisms for policy formulation and implementation;

(2) How does one effectively utilize the gamut of tools available to policymakers to combat terrorism: i.e., public diplomacy, economic and political sanctions, covert action, military force, and international cooperation and agreements;

(3) How does one prioritize for budget purposes, whatever is viewed as an appropriate mix of counterterrorism resources, to facilitate assuring that important components are neither shortchanged or overfunded depending on political "clout";

(4) How effective are sanctions and military force as policy tools; how might their use be improved; and how are commercial interests balanced in the equation. For example, how might sanctions be fine tuned or graduated to enhance their effectiveness and make their imposition more likely;

(5) What is an appropriate role for covert operations in a proactive counterterrorism policy (should the U.S. ban on assassinations be reviewed);

(6) How can one insure that the best international talent joins forces to enhance technological research and development efforts to support counterterrorism goals; and

(7) What role, if any, should the media assume in a proactive counterterrorism policy.

Also absent from the report, which largely focuses on the "stick" approach to combating terrorism, are suggestions for use of expanded "carrot" options which may moderate the behavior of rogue states or terrorist groups. Supporters of these types of incentives argue that they facilitate achievement of antiterrrorist goals without compromising core values or principles, and without giving in to the demands of terrorists. These approaches include options such as constructive engagement, creative foreign aid or trade packages, or expanded use of rewards for information programs.

For example, if U.S. trade with China is deemed to produce a moderating effect on China's rogue human rights policy, supporters of the "carrot" approach might argue that trade with Libya could have a moderating effect on that nation's rogue terrorism policy. Answers are far from clear, but pursuit of innovative "carrot"-oriented options, coupled with a strong "stick" approach, may, or may not, produce varying degrees of success in dealing with such groups as the IRA and PLO. And many still suggest that use of such options may well produce positive results with countries that seem to be moving in a positive direction such as Iran.

Conclusion

The National Commission on Terrorism's report and recommendations on countering the changing threat of international terrorism are likely to spur strong congressional interest in counterterrorism policy during the 107th Congress. The most likely areas of scrutiny include: (1) more productive counterterrorism policies and mindsets; (2) enhanced use of legislative authority to impose sanctions on states that support or actively countenance terrorism; and (3) methods of achieving a more cohesive, better coordinated federal counterterrorism effort through enhanced budget coordination mechanisms.

The United States Response to Terrorism - Is it Time to Employ the "Drug Czar" Model?

Raphael Perl and Charles Lucey, MD, JD, MPH

Introduction

Drug trafficking activity and terrorism activity have much in common. Both drugs and terrorism have strong national security and law enforcement components, they have military components, border control components, economic and trade components, medical components, and agricultural components. Today there are some 50 federal agencies with some degree of counterdrug responsibility and at least 12 federal agencies with important counterterrorism responsibilities. This paper examines one model for unifying them under an executive branch, White House director s office, as outlined below.

Drug trafficking and terrorism are illegal clandestine activities with strong national security and law enforcement threat components, and operational similarities. Terrorists like drug traffickers, need weapons and engage in violence to achieve goals. Terrorists, like drug traffickers, are often involved in hiding and laundering sources of funds. Both terrorists and drug traffickers operate transnationally, and often get logistical and operational support from local ethnic satellite communities. Both groups often rely on the criminal community for support: they may need smuggled weapons, forged documents and safe houses to operate effectively. Finally, both groups need a steady cash flow to operate. In the case of terrorists, where state sources of funding are rapidly diminishing, drug trafficking is an attractive funding option. Increasingly, terrorist organizations are looking to criminal activity and specifically the drug trade as a source of funding. The FARC (Revolutionary Armed Forces, a guerilla force) in Colombia is but one of many cases in point.

Some experts have looked to the "drug czar" model in seeking to reform government structures to fight terrorism. Counternarcotics efforts have forced local, state and federal agencies to build operable, cooperative, inter-agency relationships. The need to build and maximize similar relationships to deal with terrorism exists and some have suggested that the "Drug Czar" [White House Office of National Drug Control Policy (ONDCP)] model may have applicability to the counterterrorism arena. Legislation is currently before Congress on this issue [H.R. 4210]. It appears that the bill will not be enacted this year (2000) but will likely be reintroduced next term.

Another structural option might require that federal departments and agencies make their counterterrorism capabilities available for the efforts of the terrorism director. Such a structure could be modeled after Goldwater Nichols Department of Defense Reorganization Act. This was enacted to shape the individual military services into a more unified command structure. Under this model, the Terrorism Czar, like the commanders of the joint unified combatant commands controlling the operating forces of all four services around the world outside of the United States (CINCS) could exploit all agency counterterrorism assets on a day-to day basis, with individual federal departments and agencies tasked with developing the various counter-terrorism capabilities needed to deter, prevent, detect, and respond to terrorist activity. A potential criticism is that military command and control may not be successfully employed in civilian agencies.

The ONDCP, the so-called "drug czar s" office, is a coordinating office in the Executive Office of the President established by Congress in 1988 by P.L. 100-690. The office is charged with: (1) establishing policies, objectives, and priorities for the national drug control program; (2) promulgating a National Drug Control Strategy; (3) coordinating agency implementation of the strategy; and (4) developing, with the advice of the program managers of agencies, a consolidated national drug control budget proposal to implement the strategy that shall be transmitted to the President and Congress.

The Office is unique in the federal bureaucracy in its merging of international and domestic responsibilities in bringing together the law enforcement, intelligence, foreign policy/national security policy, and domestic health communities -- all of which are components of the counterterrorism community as well. Although the office is a policy office without an operational mandate, it does provide policy direction to operations. This is accomplished through the budget process in the form of planning guidance and recommendations on how to prepare for existing and emerging threats. By exercising its budget process review role, ONDCP performs budgetary integration of the operational aspect of interdiction activities of such agencies as the Coast Guard, the Customs Service, and the Departments of Defense and State.

P.L. 100-690 sets forth the structure of the Office and the positions requiring confirmation by Congress. By law, the appropriations process sets full-time equivalent (FTE) staffing levels at 125 slots and the office must be periodically reauthorized. Any additional FTE slot must be approved and funded by Congress. However, ONDCP has the unique power of being able to demand drug control detailees from other agencies and even to require detailee transfer of drug control personnel between or among agencies. This includes military detailees.

The Director of the Office, though not a formal statutory voting member of the Naitonal Security Council (NSC), as the President s key drug policy adviser, is the principal adviser to the NSC on national drug control policy [E.O. 12280]. The Director also chairs an interagency working group (IWG) on international counternarcotics policy charged with ensuring development and coordination of such policy. Other agencies are required by law to provide ONDCP, upon the request of the Director, with such information as may be required for drug control and the Director of Central Intelligence is specifically required by law to render full assistance and support to ONDCP.

The office develops four major documents: (1) a 10 year national Drug Control strategy supplemented by annual reports (updates); (2) an annual budget summary that includes pending budget requests and funding histories on an agency by agency basis; (3) a yearly Performance Measures of Effectiveness (PME) evaluation; and (4) a classified annex, which contains classified information on drug flow data, interdiction efforts, and emerging technologies.

The Director s budget certification power—although often unpopular with individual agencies—wields considerable clout in terms of policy input and integration. In preparing the National Strategy, ONDCP staff, in consultation with agency personnel who are often detailed to ONDCP, define the mission and the threat in terms of needs, goals and objectives. Targets and measures of effectiveness (MOE s) are established. ONDCP annually provides agencies with policy initiatives that reflect the goals and objectives of the strategy that are presumably threat driven, and that ONDCP would like to see reflected in agency budgetary priorities. Agencies respond with individual budget packages that the Director may certify as adequate to accomplish the strategy s goals and objectives. If certified, the budget goes to the President. If decertified, the agency resubmits to ONDCP. The process for resolution of disagreements usually involves the Office of Management and Budget (OMB), the White House Chief of Staff, and the Director. If not resolved, a meeting with the President, the Agency Head, an OMB representative, and the Director is scheduled. Reportedly, the last five meetings of this nature have been resolved in favor of ONDCP s position.

Supporters of the "drug czar" concept find favor in the current structure in that it permits the Director to serve as both a national and international Administration spokesperson on drug policy issues. From the congressional viewpoint, an attractive component of the drug czar model is accountability to Congress. Unlike the current counter terrorism policy/leadership structure under NSC direction, the Drug Czar is confirmed by Congress and testifies regularly before congressional committees. Moreover, when Congress reauthorized ONDCP in 1988, it enacted specific targets that the drug strategy was required to meet. Congress could consider setting targets for counterterrorism policy if it deemed this an effective approach. For those who favor a centralized coordination/control drug policy model, the Drug Czar s budget certification authority, an authority not shared by NSC staff, is seen as a favorable asset. A Director with a strong personality and strong backing from a President has been said to command the respect of a "500 pound gorilla" in the interagency community.

Others, however, suggest that the effectiveness of the Drug Czar s office in integrating the diverse and multifaceted federal counterdrug community has been mixed at best. Also, in a "czar" type structure, perhaps more so than in other bureaucratic structures, changes in leadership could significantly impair or enhance the effectiveness of a national leadership effort. Nevertheless, this area is one that might be further explored as Congress considers alternative approaches to dealing with terrorism.

Current Challenges for National Counterterrorism Efforts

A number of substantial challenges lie ahead for the counterterrorism policy community. The most prominent of these is the changing nature of the terrorism phenomenon. In past years, when terrorism was largely the product of direct state sponsorship, policymakers were able to diminish prospects for the United States becoming a target using a combination of diplomatic and military instruments to deter potential state sponsors. Today, however, many terrorist organizations and individuals appear to act independently from former and present state sponsors, shifting to other sources of support, including the development of transnational networks.

Many terrorism experts have suggested a shift in the type of violence terrorists are willing to inflict. Terrorism statistics indicate an overall reduction in the number of terrorism incidents per year, but an increase in the number of victims per incidents. While the number of historical cases of terrorists using CBRN weaponry is low, this trend toward increasing violence and less state control may drive certain terrorist groups toward unconventional weapons. On the other hand, the reduction in direct state support may decrease the terrorist s ability to acquire or independently develop CBRN weapons. These shifts have produced a number of policy and program initiatives designed to better deter and prevent future acts of terrorism while also building a national capacity to effectively respond to terrorism incidents involving the full range of weapon types.

A key challenge is working both at home and abroad to identify, track, and defeat terrorist groups before they undertake acts of violence against American citizens. Preventing terrorism requires the use of a wide array of tools for the purpose of disrupting terrorists activities by removing the secrecy they require to operate, eliminating sources of support, and prosecuting potential terrorists. Vital to the success of these efforts are on-going threat assessments. Effective threat assessment takes into account the need for abundant, timely and useable intelligence about potential terrorist sponsors, perpetrators, activities and targets, as well as intelligence in order to guide our prevention and preparation activities and programs. Despite the transnational nature of many terrorist groups, challenges to integrating foreign intelligence with domestic law enforcement information remain.

Central to threat assessment is intelligence to help develop our own targets to deter or punish state sponsors. In this regard, the development of long-term human source intelligence (HUMINT) is often cited as a vital component in building our ability to preempt attacks. Critical to threat assessment is the need to get smarter, not just in protecting against the threat from outsiders, but smarter about the threat posed by people with legitimate access. This includes acts of carelessness by insiders. A chain is only as strong as its weakest link. We need to continue our efforts to enhance our vigilance to minimize any potential threats posed by third country nationals -- for example, threats posed by outsiders working at U.S. embassies and military installations overseas.

Critical to threat assessment is a better understanding of the countries and cultures where foreign terrorists are bred and operate. This includes understanding the root causes of unrest that give rise to terrorism. It is important to understand such factors when we plan how to combat terrorist groups on an operational level. And it is important to understand such factors when planning to prevent or respond to specific terrorist attacks. Just as there is an important role for research and development in combating drug abuse, the Terrorism Czar would have overall program responsibility for prioritizing and funding in this area.

Threat assessment is an ongoing and evolving process. As the threat changes, it may do so slowly, but it may also change unexpectedly, radically, rapidly, and dramatically. To meet changing or unanticipated threats, strategies and missions may need to be modified, and allocation of resources may need to shift as well. Such circumstances require a certain fluidity of policy.

Forward-looking planning, flexibility and periodic review thus become important policy components. A community mindset that encourages the challenging of policy coupled with practical exercises designed to test policy and policy assumptions may contribute to policy relevance.

Some experts have suggested that designation of "no year" money (appropriated funds that remain in an agency s kitty, even if unspent in the appropriated year) in an agency s budget account and establishment of an interagency counterterrorism reserve contingency fund may be options that warrant consideration. This allows for greater fiscal flexibility and funding for major contingencies such as the embassy bombings in East Africa. Other experts are concerned about the lack of accountability that such a process may contain and the fact that money might be spent for purposes other than those intended.

Efforts to integrate of programs designed to improve CBRN terrorism response capacities remain disjointed and uncoordinated. While substantial progress has been made toward improving the response capacity of CBRN to a terrorism incident, these efforts have been hampered by the lack of a coordinated national strategy for building response capacity. Such a strategy should include continuous assessments of response capacity based on clearly defined measures of effectiveness for CBRN terrorism detection, assessment, and response capabilities and corresponding operational capability objectives. Based on such an on-going assessment, budgetary and programmatic priorities can be adjusted to resolve deficiencies and eliminate gaps in capabilities. As of today, there is no comprehensive budgetary process for determining counterterrorism spending that integrates current threat assessments and assessments of domestic response capabilities. In fact, it is nearly impossible to comprehensively list all government spending related to counter terrorism.

There is continuing need to sustain a credible deterrent against potential state sponsors, but also important appears to be the need to develop and sustain an increasingly proactive deterrent against terrorist groups and individuals operating independently. Involved is not only deterrence by punishment but also deterrence by denial. Moreover, developing deterrents against independent groups may diminish the probability of use of weapons of mass destruction by terrorists. Deterring potential CBRN terrorists requires close integration of various policy tools including intelligence, diplomacy, law enforcement, homeland defense capabilities, and military instruments.

One of the most important challenges facing the counterterrorism policy community is to ensure that our anti-terrorism efforts are fully coordinated. When push comes to shove, agencies still do an awful lot of ad hoc-ing. As the Oklahoma City and USS Cole bombings illustrate, terrorism is not limited to those areas in which we are prepared.

Some have suggested that policy planners need to incorporate factors relating to the impact of terrorist incidents or campaigns, not only into the domestic policy equation, but also into the foreign and defense policy equations. Some view mechanisms similar to the Defense Department s (DoD s) "Quadrennial Defense Review" as providing possible vehicles for organizing, funding, and training for antiterrorism and counter-terrorism related missions. They believe that potential contributions from such institutions as our nation s nuclear weapons laboratories to terrorism threat analysis might be more fully explored.

As we move into the first decade of the new millennium, terrorism may receive increased attention in the foreign policy, national defense, and law enforcement communities. As we assess and formulate our international and national commitments, policymakers are likely to consider the possible impacts of terrorism on those commitments and on public and political support vital to those commitments. The challenges facing us in assessing threats, allocating resources, and insuring an effective congressional role in counterterrorism policy are complex. But inherent in challenges are opportunities to bring together the diverse elements of the counterterrorism community to share information, experiences, ideas, and creative suggestions about how to effectively deal with this growing national security, law enforcement, and public policy concern.

Is Appointing a Terrorism Czar the Solution

While the drug czar strategy appears successful at meshing interagency cooperation, executive branch attention, and congressional oversight/ budgeting, has it met with outcomes to inspire confidence? Have we closed off our borders to drug smuggling? What implications might this have for narcoterrorists or others who may wish to import a Weapon of Mass Destruction (WMD) into our country? Has the Drug Czar impacted home-grown/manufactured drugs? What might that tell us about domestic terrorism? Do we need special vigilance or programs to combat biological terrorism specifically?

While there is sure to be debate regarding the answers to these questions, most can agree that drugs remain available and an important reason for our jails to be crowded. What can we learn from this? Criminals respond to technology by using any means at their disposal, ranging from low tech "mules" (who sacrifice one to allow others to get through), to a recent report of a submarine being built in Columbia that was more sophisticated than anything their government was capable of designing. Biological terrorism, known as the poor person s nuclear weapon, could fit this profile. While our customs agents have dogs and other technology to search for drugs, would they detect Anthrax powder? Does one doubt that terrorists or narcoterrorists could be motivated to carry out such a mission?

Greed and corruption know no political ideologies. Just as drug cartels have penetrated foreign governments and corrupted officials worldwide, could well-financed terrorists do the same? It would be naive to think that corrupt officials or lower level government personnel in Colombia would sell only advance information about government operations against drug cartel activity while not selling information about operations against terrorist groups. Policies are bound to fail if they do not take into account or ignore important social forces.

Many parallels exist between drug trafficking activity and terrorism. Important lessons for the counterterrorism community may lie in the Government s response to the drug trade and the way the government is organizationally structured to respond to the activities of drug trafficking organizations. Arguably, benefits of a Terrorism Czar would include better command, control, and coordination of policy and its funding and implementation (overall program responsibility). However, enhanced effectiveness will not come from organizational structure alone. A Terrorism Czar must be sensitive to ever-changing social, religious, and political phenomena spanning the globe; must be proactive, not reactive; and must keep abreast of evolving or revolutionary new technologies. The Terrorism Czar s educational activities will have to match his or her policy recommendations to keep Congress, the Executive Branch, and the American people informed and prepared. We recommend further consideration of such a model.

Acknowledgement: Mr. Michael Powers, Chemical and Biological Arms Control Institute (CBACI), and Richard Scribner, PhD, Institute for Security Technology Studies at Dartmouth College provided valuable advice and editorial assistance.

Terrorism: U. S. Response to Bombings in Kenya and Tanzania: A New Policy Direction?

Raphael F Perl

Summary

On August 20,1998 the United States launched retaliatory and preemptive missile strikes against training bases and infrastructure in Afghanistan used by groups affiliated with radical extremist and terrorist financier Usama bin Laden. A "pharmaceutical" plant in Sudan, making a critical nerve gas component, was destroyed as well. This is the first time the U.S. has unreservedly acknowledged a preemptive military strike against a terrorist organization or network. This has led to speculation that faced with a growing number of major attacks on U.S. persons and property and mounting casualties, U.S. policymakers may be setting a new direction in counter-terrorism a more proactive and global policy, less constrained when targeting terrorists, their bases, or infrastructure. Questions raised include: What is the nature and extent of any actual policy shift; what are its pros and cons; and what other policy options exist? Issues of special concern to Congress include: (1) U.S. domestic and overseas preparedness for terrorist attacks and retaliatory strikes; (2) the need for consultation with Congress over policy shifts which might result in an undeclared type of war; and (3) sustaining public and Congressional support for a long term policy which may prove costly in: (a) dollars; (b) initial up-front loss of human lives, and (c) potential restrictions on civil liberties. Whether to change the presidential ban on assassinations and whether to place Afghanistan on the "terrorism" list warrants attention as well. This short report is intended for Members and staffers who cover terrorism, as well as U.S. foreign and defense policy. It will be updated as events warrant. For more information, see CRS Issue Brief 95112, *Terrorism, the Future and U..S. Foreign Policy and CRS Report 98-722F, Terrorism: Middle East Groups and State Sponsors.*

Background

On August 7, 1998, the U.S. Embassies in Kenya and Tanzania were bombed. At least 252 people died (including 12 U.S. citizens) and more than 5,000 were injured. Secretary of State Albright pledged to "use all means at our disposal to track down and punish" those responsible. On August 20,1998, the United States launched missile strikes against training bases in Afghanistan used by groups affiliated with radical extremist and terrorist financier Usama bin Laden. U.S. officials have said there is convincing evidence he was a major player in the bombings. A pharmaceutical plant in Sudan, identified by U.S. intelligence as a precursor chemical weapons facility with connections to bin Laden, was hit as well.

The United States has bombed terrorist targets in the past in retaliation for anti-U..S. operations (Libya, in 1986 following the Berlin Disco bombing and Iraq in 1993 as a response to a plot to assassinate former President Bush) and an increasingly proactive law enforcement policy has resulted in bringing roughly 10 suspected terrorists to the U.S. for trial since 1993. However, this is the first time the U.S. has given such primary and public prominence to the *preemptive*, not just retaliatory, nature and motive of a military strike against a terrorist organization or network. This may be signaling a more proactive and global counter-terrorism policy, less constrained when targeting terrorists, their bases, or infrastructure.[1]

Is There a Policy Shift and What Are Its Key Elements?

The proactive nature of the U.S. response, if official Administration statements are to be taken at face value, can readily be interpreted to signal a new direction in anti-terrorism policy. A series of press conferences, TV interviews and written explanations given by Administration officials reveal what appears to be a carefully orchestrated theme that goes well beyond what could characterized as one-time, isolated-show-of-strength -statements. Defense Secretary William S. Cohen, in words similar to those of National Security Adviser, Sandy Berger, characterized the response as "the long term, fundamental way in which the United States intends to combat the forces of terror" and noted that "we will not simply play passive defense." Secretary of State Albright stressed in TV interviews that: "We are involved in a long- term struggle.... This is unfortunately the war of the future.." and National Security Adviser Sandy Berger stressed in public media appearances that "You can t fight this enemy simply in defense. You also have to be prepared to go on the offense". In what some see as a warning to other terrorist groups who may seek weapons of mass destruction, President Clinton in his August 20th statement from Martha s Vineyard, gave as one of four reasons for ordering the attacks :" because they are seeking to develop chemical weapons and other dangerous weapons".[2]

Statements aside, the fact remains that this is the first time the U.S. has: (1) launched and acknowledged a preemptive strike against a terrorist organization or network, (2) launched such a strike within the territory of a *state* which presumably is not conclusively, actively and directly to blame for the action triggering retaliation, (3) launched military strikes at multiple terrorist targets within the territory of more than one foreign nation, and (4) attacked a target where the avowed goal was not to attack a single individual terrorist, but an organizational infrastructure instead. Moreover, in the case of the facility in Sudan, the target was characterized as one that poses a longer term danger rather than an immediate threat.

---

1 The same day as the missile strike, the President signed an executive order E.O. 13099, [63 Fed. Reg. 45167] which would freeze any assets owned by bin Laden, specific associates, their self-proclaimed Islamic Army Organization, and prohibiting U.S. individuals and firms from doing business with them. Bin Laden s network of affiliated organizations pledged retaliation; the State Department issued an overseas travel advisory warning for U.S. citizens, and security has been heightened, particularly at embassies, airports and domestic federal installations and facilities. On August 25, 1998 it was reported a federal grand jury in New York had indicted bin Laden in June 1998 in connection with terrorist acts committed in the U.S. prior to the embassy bombings. A "retaliatory" bombing at a South African Planet Hollywood restaurant in Capetown on August 25, 1998 killed one and wounded 24 persons. For information on the role of Sudan and Afghanistan in support of International terrorism: See CRS Issue Brief 95112, Terrorism, the Future, and U.S. Foreign Policy by Raphael Perl, See also: Terrorism: Middle Eastern Groups and State Sponsors, by Kenneth Katzman , CRS Report No. 98-722 F

2 See for example: The Policy: We are Ready to Act Again, editorial by Defense Secretary William S. Cohen, *Washington Post*, August 23, 1998, p. C-1 and U.S. Hints at More Strikes at bin-Laden by Eugene Robinson and Dana Priest, *Washington Post*, p. A-1 August 22, 1998. An excellent series of excerpts from press conferences and TV interviews by Administration officials which could be used to support the premise of a policy shift are found in the PBS television series Jim Lehrer Newshour report of August 25, 1998. See also: New Rules in a New Kind of War, by Peter Grier and Jonathan S. Landay, *Christian Science Monito*r, August 24, 1998, p.1.

Inherent in Administration statements and actions are allusions to a terrorism policy which, in response to immediate casualties and a global vision of higher levels of casualties is: (1) more global, less defensive, and more proactive; (2) more national security oriented and less traditional law enforcement oriented, (3) more likely to use military force and other proactive measures, (4) less likely to be constrained by national boundaries when sanctuary is offered terrorists or their infrastructure in instances where vital national security interests are at stake, and (5) generally more unilateral when other measures fail, particularly if other nations do not make an effort to subscribe to like-minded policies up front. A policy with such elements can be characterized as one shifting from a long term diplomatic, economic and law enforcement approach to one which more frequently relies on employment of military force and covert operations. Implied in such a policy shift is the belief that though terrorism increasingly poses a threat to all nations, all nations may not sign up with *equal* commitment in the battle against it and bear the full financial and retaliatory costs of engagement. In such an environment, the aggrieved nations with the most at stake must lead the battle and may need to take the strongest measures alone.

What Are the Pros and Cons of Such a Shift?

Arguments in favor of a proactive deterrent policy. Such a policy: (1) shows strength and world leadership--i.e., other nations are less inclined to support leaders that look weak and act ineffectively; (2) provides disincentives for other would be terrorists; (3) is more cost-effective by thwarting enemy actions rather than trying to harden all potential targets, waiting for the enemy to strike, and suffering damage; (4) may truly damage or disrupt the enemy--dry up his safehavens--sources of funds and weapons and limit his ability to operate, and (5) provides governments unhappy with the U.S. response an incentive to pursue bilateral and multilateral diplomatic and law enforcement remedies to remain active players. *Arguments against a proactive military/covert operations oriented deterrent terrorism policy:* Such a policy: (1) undermines the rule of law, violating the sovereignty of nations with whom we are not at war ; (2) could increase, rather than decrease, incidents of terrorism at least in the short run; (3) leaves allies and other nations feeling left out, or endangered--damaging future prospects for international cooperation; (4) may be characterized as anti-Islamic, and (5) may radicalize some elements of populations and aid terrorist recruitment; and (6) may result in regrettable and embarrassing consequences of mistaken targetting or loss of innocent life.

What Other Policy Options Exist?

The U.S. government has employed a wide array of policy tools to combat international terrorism, from diplomacy, international cooperation and constructive engagement to economic sanctions, covert action, protective security measures and military force. Implementation of policy is often situation-driven and a military response is more likely in close time proximity to a terrorist attack when public world outrage is high and credible accountability can quickly be established. When combating non-state sponsors of terrorism like bin Laden s networks, direct *economic or political pressure* on sanctuary states and indirect pressure through neighboring states may be an effective policy tool in restricting activities and sanctuary locations as well creating a favorable climate for *legal approaches* such as criminal prosecution and extradition which is gaining prominence as an active tool in bring terrorists to trial. Working with other victim states through the U.N. and the Organization of African Unity are options which would build on the

March 1996 Sharm al-Sheikh peacemaker/terrorism summit. *Enhanced intelligence targeting* of non-state "amorphous" groups and intelligence coordination and sharing among agencies, governments, and with the private security community is critical, but mechanisms to achieve such intelligence objectives must be in place. All agree that more effective human intelligence sources must be developed. In this regard, other nations such as Saudi Arabia and Kenya may be more effective in penetrating terrorist groups than the U.S. Another option is *not to overpersonalize conflicts* against terrorist organizations and networks. Publically focusing on individuals like bin Laden (instead of on their networks or organizations) too often glamorizes such persons--drawing funding and recruits to their cause and misses the purpose of countermeasures --e.g. disabling terrorist capabilities.

Enhanced unilateral use of *covert operations*[3], though not without downsides, holds promise as an effective long-term policy alternative to high profile use of military force. A seeming industrial explosion at a factory believed to be producing nerve gas chemicals draws less formal criticism and political posturing by other nations than an openly announced missile attack. The dangers here are that the United States is not especially competent at secret-keeping and that counter-terror can be misequated to terrorism. Effective use of covert policy alternatives requires institutionalization of covert action capability tapping into the best that each agency has to offer. In a world where state sponsorship for terrorism is drying up, private funding becomes critical to the terrorist enterprise. Terrorist front businesses and banking accounts could increasingly become the target of creative covert operations. To support such efforts and effective law enforcement oriented approaches to curbing money flows, assisting personnel in other countries in tracing and stopping money flows to terrorists, their organizations and front companies may warrant consideration. So-called "grey" area or "black" area *information operations* which bring to light vulnerabilities in the personalities of key terrorist leaders (i.e .corruption, deviant sexual behavior, drug use), promote paranoia, and inter-organizational rivalries, warrant increased attention as well. One can assassinate a person physically only once; but "character assassination" in the media can be done daily.[4] U.S. terrorism policy lacks a multifaceted information offensive aspect which is not merely reactive in nature.

Issues for Congress

Issues of special concern to Congress include: (1) U.S. domestic and overseas preparedness for terrorist attacks and retaliatory strikes, (2) the need for consultation with Congress over policy shifts which might result in an undeclared type of war, and (3) sustaining public support

---

3 See: *Covert Action: An Effective Instrument of U.S. Foreign Policy?* CRS No. 96-844F

4 See: *Terrorism, the Media, and the Government: Perspectives Trends, and Options for Policymakers*, by Raphael Perl, CRS report No. 97-960 F.

for a long-term policy which may prove costly in: (a) dollars; (b) initial clearly seen loss of human lives, as well as (c) potential restrictions on civil liberties. Whether the Presidential ban on assassinations should be changed and whether Afghanistan should be placed on the "terrorism" list warrants consideration as well.[5]

An important issue brought to the forefront in the wake of the U.S. military response to the August 7, 1998 embassy bombings is that of *U.S. preparedness for domestic and overseas terrorist and retaliatory attacks*. There is no absolute preparedness; a determined terrorist can always find a soft target somewhere. Thus, advance intelligence is perhaps the most critical element of preparedness. Good working relationships with foreign intelligence services are important here. Other key elements of preparedness include: (1)the ability through law enforcement channels and covert means to actively thwart terrorist actions before they occur, (2) high profile physical security enhancement measures; (3) and the ability to limit loss of life and mass hysteria, confusion and panic in the face or wake of terrorist attacks. Particularly in situations involving weapons of mass destruction, effective mechanisms to minimize panic and ensure coordinated dissemination of critical life saving information is important, as is planning on practical matters such as how to dispose of bodies. Essential is the ability to maintain and promptly dispatch emergency teams to multiple disaster sites.

A central issue of concern is Administration *consultation with Congress over policy shifts which may result in an undeclared war*. To paraphrase a familiar congressional adage: We need to be there for the takeoffs if you expect us to support you on the crash landings. It can be argued that given the need for secrecy and surprise, and given the fact that the Administration s timing of the miliary response was dependent to large degree on the configuration of events and the activities of terrorist operatives on the ground, the Administration made reasonable efforts to inform Congress in advance of the August action to be taken as well as the targets and rationale

---

5. A key question here is whether Afhanistan should be on the terrorism list in light of the Taliban s enhanced consolidation of control over the country and its harboring of bin-Laden and associated terrorist groups, facilities, and individuals. Given the wild west nature of Afghanistan today, is it fair to hold Afghanistan liable as a viable country for state action? Also, would such action legitimize the Taliban government which so far only 3 nations have recognized? Many suggest that diplomatic initiatives and the threat of sanctions and further military retaliation against the Taliban s harboring known terrorist and supporting or countenancing terrorist training activity on their soil, will continue to prove to no avail. Should such assertions bear out, *then* a strong argument can be made that the Administration, pursuant to Section 6 (j) of the 1979 Export Administration Act (P.L. 96-72) must place Afghanistan on the Department of State s list of countires supporting terrorism list. Imposed would be restrictions of foreign aid, and severe export controls on dual use and military items. See also CRS Report 98-722F, previously cited..

of the pending missile-strike-response.[6] Notwithstanding Administration efforts to brief Congress on the attack, has the Administration been remiss in its failure to consult with and brief Congress on any new policy or major change in policy emphasis or direction? Questions for Congressional inquiry might include: What is the policy; how exactly is it different; how does it fit in with other policy options; what consequences are foreseeable; how is it to be implemented; how is effectiveness to be measured; how is it to be coordinated; what funding, organizational mechanisms or legislative authority are required to implement it effectively, and how is international support for, and cooperation in, this strategy to be pursued?

In justifying the U.S. missile response under Article 51 of the U.N. Charter (self defense), the Clinton Administration has invoked *22 USC 22377 note (otherwise known as) Section 324(4) of the Antiterrorism and Effective Death Penalty Act of 1996 P.L. 104-132]* which provides: "The Congress finds that.... The President should use all necessary means, including covert action and military force, to disrupt, dismantle, and destroy international infrastructure used by international terrorists, including overseas terrorist training facilities and safehavens". Does 22 USC 2377, as passed by Congress in 1996, amount to the counter-terrorism analogue to the Vietnam era Gulf of Tonkin Resolution? Some analysts suggest that such authority is too broad and open-ended and may pave the way for a quagmire of unconventional violent exchanges, and consequently amendment of the statute may be warranted. Others, however, feel that such broad authority is essential to allow a president maximum flexibility to counter mounting terrorist threats and stress that potential for abuse can be checked through active congressional oversight and reporting to Congress. Another issue involving presidential authority is how the presidential *ban on assassinations* (E.O. 12233) fits into any policy shift and if it should be modified or rescinded.

A more proactive terrorism policy may prove costly in dollars [even in relatively quiet times] as well as in potential restrictions on civil liberties. Unresolved questions include: (1) what is the potential dollar cost; and is the public prepared to accept the loss of lives and other consequences of such a "war of the future?" In this regard, should there be a more active federal role in public education? An informed, involved, and engaged public is critical to sustain an active anti-terrorism response. The American public will be more likely to accept casualties if they understand why they will be sustained and that sometimes it is cheaper to pay the cost up front.

---

6 According to press reports, National Security Adviser, Sandy Berger briefed Mr. Lott and Mr. Gingrich on August 19, 1998 and Mr. Gephardt s office was briefed that day. Mr. Daschle, unavailable at the time, was briefed the following day. See: Clinton gets Hill s near-solid bi-partisan support for strike, by John Godfrey, Washington Times, August 21,1998, p. A13. Also, 1/2 hour before the attacks, phone calls were placed to the Chairman and Ranking Members of the House National Security and Senate Armed Services Committees. The day after the U.S. counter-strike (August 21), Secretaries Cohen, Albright, CIA Director Tenet, and Chairman of the Joint Chief s Henry H. Shelton met with Senators and available House Members to discuss the planning and rationale of the bombings. House-focused follow up briefings are planned.

Terrorist Attack on USS Cole: Background and Issues for Congress

Raphael Perl and Ronald O Rourke

Summary

An FBI-led investigation was launched to determine culpability for the October 12, 2000 terrorist attack on the U.S. Navy destroyer Cole in Aden, Yemen. The Defense Department and the Navy initiated additional inquiries. The House and Senate Armed Services Committee held initial hearings on the incident in late October. The attack raises potential issues for Congress concerning (1) procedures used by the Cole and other U.S. forces overseas to protect against terrorist attacks; (2) intelligence collection, analysis, and dissemination as it relates to potential terrorist attacks, (3) U.S. anti-terrorism policy and how should the United States respond if and when perpetrators are discovered. This report will be updated as events warrant.

Background

On October 12, 2000, the U.S. Navy destroyer Cole[1] was attacked by a small boat laden with explosives during a brief refueling stop in the harbor of Aden, Yemen.[2] The suicide terrorist attack killed 17 members of the ship s crew, wounded 39 others, and seriously damaged the ship.[3] The attack has been widely characterized as a "boat bomb" adaptation of the truck-bomb tactic used to attack the U.S. Marine Corps barracks in Beirut in 1983 and the Khobar Towers U.S. military residence in Saudi Arabia in 1996.

The FBI, in conjunction with Yemeni law-enforcement officials, is leading an investigation to determine who is responsible for the attack. Evidence developed to date suggests that it may have been carried out by Islamic militants with possible connections to the terrorist network led by Usama bin Ladin.[4] In addition to the FBI-led investigation, Secretary of Defense William Cohen has formed a special panel headed by retired General William W. Crouch, former Vice Chief of Staff of the Army, and retired Admiral Harold W. Gehman, Jr, former commander-in-chief of U.S. Joint Forces Command, to "review applicable Department of Defense policies and procedures and address force protection matters, rules of engagement, logistical support, intelligence and counterintelligence efforts" and any other matters deemed pertinent. The Navy is

---

1. The Cole (DDG-67) is an Aegis-equipped Arleigh Burke (DDG-51) class destroyer. It was one of four DDG-51s procured in FY1991 at an average cost of about $789 million per ship. This is equivalent to about $924 million in FY2001 dollars. The ship entered service in 1996.
2. For background information on Yemen and a discussion of U.S.-Yemeni relations, see CRS Report RS20334, Yemen: Democratic Development and U.S. Relations, by Alfred B. Prados. Washington, 2000. 6p.
3. The cost to repair the ship has been preliminarily estimated at about $150 million. Funding to repair the Cole may be included in one of the final appropriation bills now being completed by Congress prior to adjournment.
4. See CRS Report No.30643, Terrorism, Near Eastern Groups and State Sponsors, by Kenneth Katzman for information on Bin Ladin s network and links to Yemen.

conducting a third inquiry into the preparations that the ship made for its refueling stop at Aden. Public hearings on the attack were held by the House Armed Services Committee on October 25, 2000, and by the Senate Armed Services Committees on October 19 and 25, 2000. Members and staff have also held classified meetings on the attack with Administration officials.

Issues for Congress

The attack on the Cole raises potential issues for Congress concerning (1) procedures used by the Cole and other U.S. forces overseas to protect against terrorist attacks; (2) intelligence collection, analysis, and dissemination as it relates to potential terrorist attacks; and (3) U.S. anti-terrorism policy and how the U.S. should respond to this attack. These issues are discussed below. Force-protection procedures. Before it arrived at Aden for its brief refueling stop, the Cole, like all visiting U.S. ships, was required to file a force-protection plan for the visit. This plan was approved by higher U.S. military authorities, and was implemented during the ship s visit. In accordance with the plan, the Cole at the time of the attack was operating under threat condition Bravo, which is a heightened state of readiness against potential terrorist attack. (The lowest condition of heightened readiness is Alpha; Bravo is higher; Charlie is higher still, and Delta is the highest.) This threat condition includes steps that are specifically intended to provide protection against attack by small boats.

Members of the House and Senate Armed Services committees and other observers have raised several issues concerning the force-protection procedures being used by the Cole and by other U.S. military forces and bases in the region, including the following:

- What were the elements of the Cole s force-protection plan and how were these elements determined?

- Did the Cole effectively implement all the elements of this plan? If not, why not? If so, does this indicate that the plan was not adequate for defending against this type of attack?

- Was the force-protection plan, including the use of threat condition Bravo, appropriate in light of the terrorist threat information that was available to military officials in the days leading up to the ship s visit? Was the ship s threat condition consistent with the very high threat condition being maintained at that time by the U.S. embassy in Yemen?

- What changes, if any, should be made in force-protection policies for ships and other U.S. military forces and bases overseas, particularly in the Middle East and Persian Gulf region? Given the need for Navy ships to periodically refuel and receive other services from local sources, as well as the potential difficulty of identifying hostile craft in often-crowded harbors, how much can be done to reduce the risk of future attacks like this one? What can be done to protect against more sophisticated terrorist tactics for attacking ships, such as using midget or personal submarines, scuba divers with limpet mines, or com mand-detonated harbor mines? Should the Navy reduce its use of ports for refueling stops and instead rely more on at-sea tanker refuelings? How many additional tankers, at what cost, might be needed to implement such a change, and how would this affect the Navy s ability to use such stops to contribute to U.S. engagement with other countries?

In addition to these issues, members of the House and Senate Armed Services committees at the hearings also raised an underlying question on whether the Cole s refueling stop was necessary from an operational (as opposed to political/diplomatic) point of view.[5]

Intelligence collection, analysis, and dissemination. Members of the Armed Services and Intelligence committees as well as other observers have raised several questions relating to the role of intelligence collection, analysis and dissemination in the Cole attack and in preventing other terrorist attacks against the United States. In some cases, these questions have been spurred by press reports about the existence of information and analyses from the U.S. Intelligence Community that, some argue, might have helped prevent the attack had it been given greater consideration or been disseminated more quickly.[6] The details of these claims are currently under investigation by the Executive Branch and Committees in Congress. Questions include the following:

- Does the United States have sufficient intelligence collection capacity, particularly in the form of human intelligence (as opposed to intelligence gathering by satellites or other technical means), for learning about potential terrorist attacks, particularly in the Middle East or Persian Gulf? Does the attack on the Cole represent a U.S. intelligence failure, or does it instead reflect the significant challenges of learning about all such attacks soon enough to head them off?

---

5. Defense Department officials testified that the refueling stop was necessary operationally because the Cole was making a 3,300-mile transit from the Mediterranean (where it previously refueled) to the Persian Gulf. Arleigh Burke-class ships like the Cole have a published steaming range of 4,400 miles at 20 knots. Transits are typically made at 14-15 knots, and steaming reange at these speeds is greater than at 20 knots. It thus appears that the Cole could have transited to the Gulf with 25 percent or more of its fuel to spare. Defense Department officials, however, state that it is Navy policy to keep its forward-deployed warships fueled to not less than 50 percent of capacity, aparently to preserve their tactical mobility in the event of an emergency. The Cole was projected to be at about 53 percent fuel when it reached Yemen, and while there were two tanker ships in the Mediterranean and one in the Persian Gulf, there were none in between Some officials have inquired as to whether the unavailability of a tanker near Yemen is a consequence of the reduction in size of the Navy during the 1990 s. Defense Department officials argue that this point is moot because it has never been Navy policy to assign tankers so that one could always be assigned to combat ships engaged in solitary transits. Since the end of the Cold War, though, the Navy has become more comfortable with the idea of breaking forward-deploying battle groups into small sub-formations, including solitary ships, to take better advantage of the modular flexibility of naval forces for responding to specific needs overseas. The policy issue might thus be as follows: Are the refueling-related risks created by (possibly-more-frequent) solitary transits combined with the 50-percent fuel policy properly balanced against the benefits of moving ships in this manner and preserving their projected tactical mobility upon arrival at the intended area of operation?

6. See for example, Scarborough, Rowan. Pentagon Analyst Resigns Over Ignored Warnings. Washington Times, October 26, 2000: A1; Becker, Elizabeth, and Steven Lee Myers. Pentagon Aide Quits, Warnings Ignored, He Says. New York Times, October 26, 2000; Suro, Roberto, and Vernon Loeb. U.S. Had Hints of Possible Attack. Washington Post, October 26, 2000: A32; Gertz, Bill. NSA s Warning Arrived Too Late To Save The Cole. Washington Times, October 25, 2000: A1.

• In the days and weeks prior to the attack on the Cole, was all the available intelligence information about potential terrorist attacks in the Middle East and Persian Gulf given proper weight in U.S. assessments of the terrorist threat in that region? Were reports pro viding information and analyses of potential terrorist attacks in the region disseminated on a timely basis to U.S. military and civilian officials in the region who have responsibility for providing advice or making decisions about ship refueling stops or other military oper ations?

• Was there adequate coordination, prior to the attack on the Cole, between the Defense Department [including the National Security Agency], the State Department, and the U.S. Central Command (the regional U.S. military command for the Middle East and Persian Gulf) in sharing and using available intelligence information and analyses on potential ter rorist attacks?

• What actions, if any, should be taken to improve U.S. intelligence collection and analy sis, particularly as it relates to potential terrorist attacks on U.S. assets in the Middle East and Persian Gulf or elsewhere?

U.S. anti-terrorism policy and potential response. Beyond these more specific issues, the attack on the Cole poses several additional potential issues relating to U.S. anti-terrorism policy in general. Some of these issues highlight dilemmas and concerns inherent in policies designed to prevent or mitigate terrorist acts. These issues include the following:

Why was Yemen chosen for refueling? U.S. Navy ships began making refueling stops in Aden in January 1999. Since then, Navy ships have stopped there 27 times to refuel, twice to make port visits, and once to take on supplies. Members of the Armed Services Committees and other observers have asked why the U.S. Central Command decided in 1998 to begin using Yemen for refueling stops rather than continuing to use nearby Djibouti on the Horn of Africa (which U.S. Navy ships had used for refueling for several years) — and why Central Command continued to use Yemen this year for refuelings when an April 2000 State Department report on worldwide terrorism characterized Yemen as a haven for terrorists but did not mention Djibouti. Members and others have asked whether the risk of a terrorist attack against a U.S. ship in Yemen was properly balanced against the political/diplomatic goals of improving relations with Yemen and encouraging its development toward a stable, pro-Western, democratic country that does not support terrorism and cooperates with U.S. efforts to contain Iraq. In response, General Tommy R. Franks, the current Commander-in-Chief of U.S. Central Command, stated the following regarding the process that led his predecessor, General Anthony C. Zinni, to the decision to use Yemen for refueling stops:

> The decision to go into Aden for refueling was based on operational as well as geo-strate gic factors and included an assessment of the terrorist and conventional threats in the region. As you know, the Horn of Africa was in great turmoil in 1998. We had continu ing instability in Somalia, the embassy bombings in Kenya and Tanzania, an ongoing war between Ethiopia and Eritrea, and an internal war in Sudan....As of December 1998, 14 of the 20 countries in the USCENTCOM AOR [U.S. Central Command area of responsibil

ity] were characterized as "High Threat" countries.

> Djibouti, which had been the Navy refueling stop in the Southern Red Sea for over a decade, began to deteriorate as a useful port because of the Eritrea-Ethiopia war. This war caused increased force-protection concerns for our ships, as well as congestion in the port resulting in operational delays. The judgment at this time was that USCENTCOM need ed to look for more refueling options, and Aden, Yemen was seen as a viable alternative. At the time the refueling contract was signed, the addition brought the number of ports available in the USCENTCOM AOR to 13. Selection of which of these ports to use for a specific refueling operation involves careful evaluation of the threat and operational requirements.

> The terrorism threat is endemic in the AOR, and USCENTCOM takes extensive measures to protect our forces.... The threat situation was monitored regularly in Yemen and throughout the AOR. The intelligence community and USCENTCOM consider this AOR a High Threat environment, and our assessments of the regional threat and the threat in Yemen were consistent in their evaluation. We had conducted a number of threat assess ments in the port, and throughout the area. However, leading up to the attack on USS Cole on 12 October, we received no specific threat information for Yemen or for the port of Aden that would cause us to change our assessment. Had such warning been received, action would have been taken by the operating forces in response to the warning.[7]

Anticipating new modes of terrorist attack. Truck bombs have been used to attack U.S. targets for at least 17 years. Did U.S. intelligence and counter-terrorism agencies anticipate or consider sufficiently plausible the possible use of the maritime equivalent of a truck bomb against a U.S. Navy ship in a harbor? If not, what changes, if any, should be made to improve the ability of U.S. intelligence and counter-terrorism agencies to identify and give sufficient prominence to modes of terrorist attack that have not been previously used? Should U.S. officials reach out more to non-governmental organizations and individuals for help in this regard?

Protecting against threats posed by persons with legitimate access. What is the best way to defend against terrorist attacks by persons with legitimate access to U.S. installations or forces? The Cole was refueled by a private Yemeni ship supply company that had advance information on the ship s itinerary. Although it now appears that the attack may have been carried out by persons with no connection to this firm, the attack still raises questions about the security implications of relying on private foreign companies to refuel U.S. Navy ships. What steps can be taken to reduce the risk posed by relying on such firms? Should, for example, the State Department s Anti-Terrorism Assistance program (ATA) be enhanced so that it can better assist foreign governments, when needed, in personnel screening and security procedures?

---

7. Opening Remarks of General Tommy R. Franks, Command In Chief, U.S. Central Command, Before the United States Senate Armed Services Committee, 25 October 2000. This statement is posted on the Web page of the Senate Armed Services Committee under the hearing in question.

The role of the FBI in counter-terrorism. Some observers have asked whether (or under what circumstances) it is appropriate for the FBI, traditionally a domestic U.S. law-enforcement agency, to take a de facto lead role in overseas investigations of terrorist attacks. Although the FBI s investigative skills are critical to such investigations, some observers argue that other skills outside the FBI s area of specialization, including having an in-depth understanding of foreign countries and cultures and the diplomatic ability to ensure host nation cooperation, are equally important components of such investigations. Clearly, small nations may feel overwhelmed by large numbers of FBI agents and the political sensitivities of their insistence on questioning local witnesses/suspects. Conferees on the FY 2001 Foreign Operations Appropriations bill [HR4811] made $4 million for counterterrorism training in Yemen contingent on FBI certification that Yemen is fully cooperating in the Cole investigation.

Insuring coordination of any retaliatory response. An important challenge facing U.S. counter-terrorism officials is to ensure that U.S. actions for military/economic retaliation for terrorist attacks are adequately planned. The need for maintaining secrecy in planning military actions can discourage interagency coordination, which in turn can create a potential for making a planning mistake. Some observers argue that the U.S. cruise missile attack on what some believe was a legitimate pharmaceutical factory in Sudan in response to the 1998 embassy bombings in East Africa was a mistake caused in part by lack of interagency coordination that deprived decisionmakers of important data which might have influenced the target-selection process.[8] If it is determined that the attack was linked to Bin Ladin, a major issue is how the U.S. responds and prevents further attacks from a network that is believed responsible for several anti-U.S. attacks since 1992. The U.S. retaliatory attack on Afghanistan in August 1998, a response to the East Africa Embassy bombings, did little to damage Bin Laden s network or his ability to plan attacks.

---

8. For a discussion of the bombing response and its policy implications, see CRS Report 98-733, Terrorism: U.S. Response to Bombings in Kenya and Tanzania: A New Policy Direction? By Raphael Perl. Washington, 1998 (September 1, 1998) 6p.

Operational Plans and How they are Influenced by Emerging Technologies

Joseph Rosen, MD

Operational plans are designed to implement policy and strategy. They provide the guidelines that operators use to respond to their tasks. If the policy is not functional, then it is unlikely that a good operational plan can overcome its faults. Emerging threats can cause major dysfunctions in our policies and strategies; these will render current operational plans unable to meet the tasks that they are expected to accomplish.

Present policies or counterterrorist policies that are based upon unrealistic assessments of the biothreats will result in operational plans that are not prepared to address the magnitude of a potential attack on our society. We have specifically chosen a combined bioweapons attack followed by a cyberattack for our discussion because it creates a discontinuity between the present Federal Response Plan s approach and the nature of the threat that is posed to our society. This gap will continue to exist unless a process is put in place to address present and future emerging threats that create discontinuities between response plans and the threats that they are tasked to treat.

Operational plans are the working documents that enable each of the groups and agencies tasked in responding to a terrorist attack to effectively carry out US policy on counterterrorism. As described in the Terrorism Incident Annex to the Federal Response Plan implementing PDD-39 the FBI is the lead federal agency in crisis management and FEMA is the lead federal agency in consequence management. The FBI on-scene commander will coordinate local responders and when the crisis is overcome FEMA will take charge. In addition to the Federal Response Plan, each state has its own plan for terrorist attacks. We have reviewed five of these plans and include this paper in our executive summary. We have also included details of several of these plans in our edited volume for a more in depth evaluation.

These inter-agency plans co-ordinate local responders with federal agencies from both the justice and defense departments. (They co-ordinate, when needed, to respond to attacks that involve multiple states.) When the attack involves mass casualties from a bioweapon attack, they instruct HHS and CDC to respond to the mass casualties and to the bioagent that was used in the attack. In theory, the plans are well thought out and will work effectively in the event of a large-scale attack on an American city.

The goal of this report is to understand how emerging technologies will affect the operational plans from the standpoint of emerging threats and emerging responses to these threats. The individuals that are tasked to respond to these attacks are trained and experienced in conventional tactical attacks that are limited to an event that is directed at one site. Most events in the past have been from conventional explosive devices, and although they have caused mass casualties, the event has been contained. The FBI has managed the crisis and in most cases apprehended the terrorists. FEMA has managed the consequence once the crisis is over.

Emerging technologies that create bioweapons that infect large segments of the population, spread rapidly, have latency, allow release in the air, and are relatively inexpensive to produce, present an attack that may overwhelm present inter-agencies plans. These events will need a level of co-ordination and training that has not been achieved in the past. It differs from a conventional attack with an explosive device; the rapid spread of the disease would require rapid containment and quarantine of large populations across multiple states and cities. Although most bioagents today have treatments, we expect that with biotechnology, after 2005 there will appear a new assortment of bioagents for which we do not have treatments. We also expect that by 2025 with genetic engineering there will be a more dramatic change in these agents making them harder to detect and treat.

Emerging technologies that respond to these bioagents will lag behind the new bioweapons. We believe that emerging technologies can be used to create new types of vaccines and treatments, but ultimately we must rely on an operational plan that limits the spread of those infected and allows a rapid quarantine to take place. When possible, the operational plan will need to include a method to dispense treatments to mass casualties, which could be as much as 10% to 30% of the population when an area has been contaminated and the first responders themselves become victims. It should also be noted that in a bioweapon attack the first responders are not law enforcement, but rather medical personnel. These personnel are often not trained in how to respond to a mass casualty event. Hospitals are already filled to capacity. Many medical personnel will not respond if they know that they have a high chance of becoming casualties. A remote tele-operated response may be ideal in a situation such as this.

The special case of a bioweapons attack is a severe test of our operational plans and requires a training environment in which we can practice how best to operate this type of response. It will not be possible to learn how to do this once the event has occurred, and the FBI will have to rely on other agencies to step in to deal with the ongoing medical situation. In addition, and most importantly, a bioweapons attack can be a strategic attack when certain bioagents are used. These agents are well known, and would create a situation that may cause a collapse in our society if the attack is successful and not rapidly contained by our operational plans.

We have used emerging technologies to create a special approach to a bioweapons attack that involves a rapid spread of an infection to multiple cities. Although our approach would not prevent the attack, it would help to contain its effects to prevent it from moving from a tactical attack to one that would be of strategic consequence. Although the present federal response plan is likely an effective approach against tactical terrorist threats, we believe that strategic weapons may overwhelm it.

We also see an opportunity for a cyberthreat in conjunction with a biothreat to be used as an emerging terrorist threat. Any major biothreat now and especially in the future, would put great demands on the computer based information systems that hospitals use. Such a system would not likely be able to handle a biothreat and could collapse through increased demand. It is also possible that clinical information systems, that will be more and more computer-based in the future, could also be infiltrated. This would rapidly and dramatically interfere with our ability to contain a bioattack.

Our goal is not to present an overwhelming doomsday scenario. We believe that there are effective methods to prepare for this worst-case scenario and that this preparation will help us test our present interagency plans. It will provide an opportunity for the many agencies to evolve and strengthen their present plans, better coordinate the response teams, and integrate first responders and federal agencies from both the justice and defense departments. It is important to bring together policy makers and technologists in these training sessions so that they may learn or contribute to the operational plans before the plans are put into action.

Challenges In Coordinating The Response To Bioterrorism

Michael S. Ascher

The overall impact of a bioterrorist attack will be determined by the balance between factors inherent in the threat organism (infectivity, pathogenicity, communicability, and antibiotic susceptibility) and the response of the public health system (disease detection, organism identification, antibiotic therapy or immunization, and environmental mitigation). Although organism factors can be anticipated and responses tailored to likely possibilities, it is clear that organisms can be engineered to escape conventional measures. This is a serious problem in its own right, but the larger issue that the community must face is that the myriad components of the response system are very poorly organized at this time. Unless this situation is rectified, in a real event, a fragmented and incomplete response would likely occur with clear adverse consequences on the public's health.

The reasons for the failure of coordination of the response system are numerous. First, as highlighted in the recent National Commission on Terrorism report, is the absence of overall Federal leadership to coordinate funding, to ensure total coverage and to prevent duplication. At present, one component may feel that its activities are appropriate, yet it maybe merely duplicating another independent entity's mission, and leaving major gaps in the overall system. One example is the focus by the National Guard Civil Support Teams on developing field laboratory capability for biological threats while at the same time the U.S. Public Health Service, through the CDC, has an initiative to make state-of-the-art laboratory testing available on short notice to any jurisdiction within the U.S. These two programs are just beginning to talk to each other and it is not clear that the National Guard program will be required at all once the CDC program is up and running. While this duplication of activities in the laboratory arena has occurred, neither the CDC nor the National Guard has begun to think about systems to actually deliver and administer therapeutics to the site of an event. This is clearly the most serious hole among several in the overall response plan.

A second major challenge in coordinating the response to bioterrorism that most workers in the field are familiar with is defining the role of traditional "first-reponders." Fire, police, Emergency Medical Services and HAZMAT capabilities are, of course, the key to the response to an explosive or chemical incident. Their roles in a bioterrorist event, which presents as an epidemic of disease, are not clear. The problem is that much of the planning and most of thefunding has been provided under a scheme in which "bio" is just a variant HAZMAT threat, a "living chemical", if you will. The clearest example of this problem is the Office of Justice Programs equipment grant program. Under the guidance of the Defense Department's former chemical defense program, local jurisdictions are required to purchase a set of equipment to be in compliance with the program. The specified HAZMAT suits and training are obviously appropriate for chemical threats but their utility in a biologic event is not clear. Additionally, without consultation or guidance of the best biodefense programs in the military, hand-held rapid test kits were (and are still being) provided to fire, police, EMS, and HAZMAT units. These kits have not been validated for this purpose and anecdotal experience suggests that they are not at all useful because of problems with both false-negative and false-positive results. Add to this the National Guard laboratory program discussed above, the plans of the FBI to deploy "flyaway" laboratory capability and the Marines' CBIRF plans and we can visualize a five-player laboratory response at an incident site. Since these programs are totally independent and turf-conscious, there has been little or no coordination or cooperation between them up to this point. Although the politics of correcting this situation are quite involved, the simple problem for a local jurisdiction is that chaos would ensue if all these laboratory resources were to descend on an incident site without careful advance planning.

There are parallels in the other component activities such as disease surveillance and emergency medical response where multiple Federal, State, and local initiatives are disconnected from each other. As referenced in the recent report of the National Committee on Terrorism, until overall planning, including all budgets, are under the control of one party, chaos will continue to reign. A further political problem occurs when the group that might be considered most critical to the response to bioterrorism, public health, tries to get attention and funding from government sources. Congress almost certainly believes that the combination of the Nunn-Lugar-Domenici funding, the National Guard program, the National Disaster Medical Systems, the U.S. Marines CBIRF, the CDC program and the FBI "flyaway" program must be able to deal with a crisis. If all these pieces had been designed from the start to fit together and forced to work together, that might indeed be the case, but instead we have duplicative programs with large holes remaining.

One further example is worthy of consideration. The U.S. military overall possesses considerable capability in the area of medical care in field situations. However, with the recent downsizing and realignment of resources within the Army, the majority of medical assets are in the Reserve component and the National Guard no longer has hospitals or medical personnel capable of providing care in an emergency situation. Nevertheless all the funding and responsibility for the military's support role thus far have gone to the National Guard, which no longer has the resources necessary to respond to an incident. It is unclear if the funders in Congress are aware of this fact. In the face of this situation, the military has changed its warfighting doctrine to state that all actions in the future will require the coordinated response of active, reserve, and guard units, the so-called "multi-compo" response. This obviously appropriate change in policy has not filtered down to the planning for the civilian response to bioterrorism, and it is unclear if it ever will, mainly for political reasons.

In conclusion, there are major challenges in coordinating the myriad of resources that are available to respond to a bioterrorist event. Duplication of effort is prominent and major gaps remain to be filled. Given that there appears to be no leadership on the Federal level on this issue, it will be up to the states and local jurisdictions to develop and organize the response capability on their own. This is clearly not the best way to prepare for bioterrorism on a national level and every effort must be made to correct this situation.

Summary of Five State Emergency Response Plans for Biological Terrorism

Charles Lucey, M.D., J.D., M.P.H.

Responsibility for preparing and responding to a biological terrorist even rests upon the States and local first responders. In May 2000, the TOPOFF (top officials of U.S. government) exercises were held to test the nation s ability to respond to simultaneous attacks on 3 municipalities, using a biological, chemical, or radiological weapons of mass destruction (WMD). In, "A Plague on your city: observations from Topoff," (http://www.hopkinsbiodefense.org/pages/news/quarter.html), Inglesby, Grossman, and O Toole review the biological attack scenario, played out in Denver, Co. In this exercise, plague (Y. pestis) bacilli was covertly released at the Denver Performing Arts Center.

In the four days of the exercise, strengths and weaknesses of present response planning could be identified. Scenario planners inserted data in response to participant actions, allowing the infection to spread to multiple locations, involving neighboring states and other nations. Secondary infection was possible for anyone, not protected with a dust mask, who came within 6 feet of a coughing person. The end result was an overextended and exhausted health system, including hospitals, public health, antibiotic distribution, and so forth. Command and control difficulties were identified, including difficulty communicating by telephone, as many responders could not be found in their offices. Concerns were raised about maintaining public order, triaging the "worried well," and coordinating responders who had never worked together. There was difficulty containing the spread with quarantine measures and supplying the population confined to their homes. The exercises showed how far we have come in our efforts and how far we still have to go. A handful of states were contacted to survey local response planning.

The California Terrorism Response Plan (December, 1998) is an annex to the state emergency plan and is currently undergoing revision. The plan is written in conjunction with federal plans, as described in the California-Federal Emergency Operations Center Guidelines. It states that the Governor has the emergency authority to plan for, procure, and pre-position supplies, medicines, materials, and equipment to mitigate the possible effects of an emergency. The Governor may activate emergency organizations in advance of an actual emergency, if prewarned.

California relies on its Standardized Emergency management System (SEMS) for responding and managing multi-agency and/or multi-jurisdictional emergencies and disasters. SEMS incorporates the Incident Command System (ICS), the California Master Mutual Aid Agreement, and an Operational Area concept (state counties). Each Operational Area operates its own emergency response plan and facilities communication among all local governments. The person in charge may be a fire chief, sheriff, or other local official as designated by the county. He or she can request help from a Regional Emergency Operations Center when needed. Cities and counties have primary responsibility for protecting local citizens when an event happens.

The State Standing Committee on Terrorism meets quarterly to provide advice and rapid consultation should the need arise. Members include state and federal agency officials plus visiting experts invited by the committee. They have an advisory and coordination role, ceding crisis management to the FBI while exercising preeminent authority to make decisions regarding consequence management. California s experiences with natural disasters has given it a practical foundation with the governor s office directly overseeing future response planning.

The Maryland Strategic Plan to Improve the Health and Medical Response to Terrorism, (February 23, 2000, http://miemss.umaryland.edu/Home.htm), lists twelve key assumptions /planning principles. The first is that planning for a WMD event will be based upon the existing system for handling a mass casualty incident rather than special purpose plans. Their planning will be based on 1000 live victims. From time of detection, state and local responders may need to wait up to thirty-six hours for federal assistance. It states hat preparedness for biological events relies on early detection, surveillance, and monitoring capabilities that are minimal at best, are not well-coordinated, and will require intelligence and data transfers between health, medical, law enforcement and others that do not currently have the ability to share and transfer information and intelligence. Pre-positioning and deploying health and medical detection, diagnostic and treatment resources will require mutual aid between jurisdictions and public and private entities that may not have existing relationships. Other points cover coordination with federal plans and effective state communication and command structure.

The Maryland Health and Medical System Preparedness and Response Plan- Weapons of Mass Destruction (draft work plan), dated May 10, 2000, provides a greater level of detail to the Strategic Plan, above. It is a product of three focus group efforts: emergency medical services, hospitals, and public health. It also represents the partnership of three government agencies:

- Maryland Emergency Management Agency (MEMA)
- Maryland Department of Health and Mental Hygiene (DHMH)
- Maryland Institute for Emergency Medical Services Systems (MIEMSS).

This report states that no Maryland hospital emergency department can handle a mass casualty incident numbering the hundreds. No regional group of hospitals can handle a 1000 live casualty surge ("catastrophic event"). The report frankly states that Maryland is unprepared for a catastrophic event and that a WMD agent will produce a casualty rate, which will rapidly overwhelm the health care emergency response system. To estimate bed availability for such an event, they started with the average daily census and calculated 20% could be rapidly dedicated to casualty care.

The Maryland State Police will act in support of the FBI for crisis management. The Maryland Emergency Management Agency is the lead State agency for consequence management. The plan proposes that each acute care general hospital maintain a disaster cache sufficient to treat hundred victims for seventy-two hours. It suggests that each local health department maintain a medication cache to treat hundred victims for seventy-two hours. Hospitals and local health departments will coordinate on how to maintain fresh supplies/medications.

Each hospital will be capable of decontaminating five patients per hour. Emergency communication and paging systems will be capable of transmitting alert messages. Encrypted electronic, real time, Internet communication shall connect the lead agencies, the twenty-four local health departments, hospital emergency rooms, infection control programs, and so forth. MEMA is to maintain an Incident Response Team to assist local governments with assessments and response.

The State of Oklahoma Emergency Operations Plan (March 10, 2000) begins with a basic section, which covers the concept of operations. It assigns the Director, Department of Civil Emergency Management, to direct, control, or coordinate all interagency and volunteer service organizations operations. The Director will also be the Governor s Authorized Representative for FEMA coordination. It directs that each identified agency provide 24-hour capability to provide a liaison officer to the State Emergency Operations Center as required by the Director. It provides a line of succession and gives citations to state and federal laws and directives.

The plan has seventeen appendices which review needs for areas such as transportation, health/medical, communications, and so forth, including #17, terrorism preparedness. Each section covers purpose, situation and assumptions, concept of operations, and organization and assignment of responsibilities. Each is fairly brief; terrorism preparedness is seven pages and does not have a section devoted to biological terrorism.

The State of Texas Emergency Management Plan (December 17, 1999) addresses all disasters, natural or man-made, without specifically addressing biological terrorism. The plan states that each agency under the plan is to develop its own comprehensive standard operating procedures, training, and periodic exercises. The plan covers four phases of emergency management: mitigation, preparedness, response, and recovery.

The plan assigns primary responsibility to local emergency operations, with state resources committed upon request of local officials. If state operations are damaged or overwhelmed, federal assistance will be relied upon. The state organizes its resources at the local level with a Disaster District Committee that supports functional groups known as emergency support functions (ESF). Each EST consists of a primary agency and support agencies best equipped to manage an emergency. These support services could be veterinary, mortuary, potable water, etc. There is an Emergency Management Assistance Compact for interstate mutual aid that the Governor can activate.

State Disaster Districts parallel those of the Department of Public Safety (DPS) Highway Patrol, dividing the state into manageable areas. Regional Liaison Officers from the Governor s Division of Emergency Management are assigned to each DPS region. The Governor has the power to wave state rules that might hinder disaster management. He or she has the power to use all available state resources and may reassign state personnel. He or she may commandeer private property, subject to compensations requirements. The Governor can prescribe evacuation, control movement of persons and occupancy, and manage debris on private lands if it threatens public health or safety.

The Governor has designated the Director of DPS as the Chairperson of the State Emergency Management Council, who in turn appoints a state coordinator for day-to-day management. This coordinator also has responsibility in Texas for managing the state drought plan. The Emergency Management Council is composed of the heads of state agencies, the American Red Cross, and The Salvation Army. Each department designates three individuals to serve as 24-hour contacts. The plan reviews the responsibilities of agencies, lines of succession for the executive, legislative, and judiciary branches, readiness levels, emergency support centers, and lists state plan annexes, including one for terrorism.

There is also a fill-in-the-blank annex for local planners to use for terrorism response planning. Two pages specifically address biological agents. The Department of Health and Hospitals maintains plans for emergency medical management. A web site exists to provide most annexes and coordination at www.txdps.state.tx.us/dem.

On October 18, 2000, the Vermont Association of Hospitals & Health Systems, the Vermont Army National Guard, Vermont Department of Health, and Vermont Department of Public Safety- Emergency Management Division held a full day seminar to review "Statewide Medical Disaster Planning and Preparedness." Along with presentations from these organizations, a representative of the U.S. Public Health Service reviewed federal response plans and an outside guest speaker gave another state s perspective on planning WMD response.

Vermont is working on developing a biological terrorism response plan. It has implemented an interhospital mutual aid response agreement to better coordinate for all emergencies. This includes an effort to coordinate with facilities outside of Vermont and to allow emergency licensing of health professionals from other states and Canada (licensing regulations under development). The local fire chief (many are volunteer) is in charge and can request state aid. The state does maintain 24-hour emergency responsiveness and trains local 911 systems on points of contact. It will coordinate closely with the federal plan. Most counties do not have public health clinics. This was Vermont s first conference on medical disaster planning and many questions were posed by the participants on state and federal regulations, such as how federal patient transfer rules might need to be violated during an emergency. Facilities, including the regional veterans hospital, reported opting out of HAZMAT decontamination capability, due to OSHA, EPA, and other agency costly regulations.

Conclusion

In this time where The Boston Globe s lead story is "More ERs diverting patients," (October 31, 2000), reporting that Massachusetts General is averaging forty-five hours per week of not accepting ambulances, where West Nile Virus has spread to other eastern states, where Ebola virus has new outbreaks, and terrorists kill seventeen on a billion dollar Navy ship, there is a credible biological terrorism threat that the U.S. and the states must prepare for.

Richard Hutchinson, Ph.D., U.S. Army, Soldier and Biological Chemical Command, has recommended planning for a range of casualties from 0.1% to 10% of the city or area population. The worried well may inflate those levels further by a multiplier of up to 5. This range is based on (1) past U.S. vulnerability simulation trials, (2) the actual levels of future biological attacks are unknown and cannot be predicted, and (3) a response strategy that can cope with such a range of casualties should be robust enough to deal with any actual event. Medical experts from CDC have indicated that the country needs to prepare for a natural pandemic involving high levels of casualties such as the 1918 flu outbreak. It seems prudent for state plans to handle casualty levels in the 10,000 to 100,000 range.

Pre-planning medical capabilities with respect to functions, locations, personnel and supply requirements is critical to establishing a flexible emergency response contingency capability. These contingency capabilities can expand in a modular manner using the existing medical system of area hospitals, clinics and local emergency response assets. While local resources cannot fully establish or man these capabilities during a biological incident infecting 10% of the population, they could initiate all of these capabilities into which State, regional and Federal assets could effectively supplement. Such planning for overmatched local resources should anticipate a structure to coordinate and command the area medical assets for maximum patient care efficiency. (The need for such unified medial command was identified by the participating hospitals during the recent TOPOFF exercise in Denver.)

In my informal survey of a handful of states, inquiries were made to Colorado, New Hampshire and New York to obtain state plans specific for biological terrorism. They were unable to provide them, stating that they were in draft currently. States are performing needs assessments as part of the Department of Justice s grants process for improving terrorism response planning. Important progress is being made but our informal review suggests that efforts cannot let up to improve local preparedness.

Examining the Military and Law Enforcement Terrorism Counteraction Model: A Template for Medical Response to Biological Terrorism?

William L. Bograkos and Daniel J. Kaszeta

Introduction: The greatest emerging biological threat is not a particular pathogen or toxin, nor is it a novel method of dissemination. It is the lack of cogent emergency planning. The United States government has expended significant funds and effort to increase the preparedness of local, state, and federal agencies to respond to incidents involving Weapons of Mass Destruction (WMD). Preparedness efforts have been following different paths and thought processes among the key response communities: fire/hazmat, law enforcement, EMS, public health, hospitals, and the military. Although the government devotes much effort to training and exercises, there is a paucity of consistent and useful planning guidance that is applicable across the community, particularly for hospitals and medical professionals. Clearly, hospitals and physicians are the front line in the defense against biological terrorism, a reality that is not consistently realized among policy makers. This paper proposes a common template for preparedness for biological terrorism. Our intent is to propose a conceptual model that can be useful to both the medical and law enforcement communities.

***Terrorism*:** For purposes of discussion, we shall use the Department of Justice and FBI definition of terrorism. A terrorist incident is "a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives."[1] Counterterrorism is the range of offensive action taken against terrorist groups or individuals, while antiterrorism is the spectrum of defensive actions taken to protect against an act of terrorism.

***7-step Counterterrorism Model*:** In the early 1980's, the United States Army developed a conceptual model to prevent, deter, and respond to acts of terrorism. This model represents both a process for planning for specific acts, and a thought process that can guide preparedness efforts (See Figure1). The seven-step model reflects primarily military and law enforcement thinking. Strictly speaking, given that the terms and definitions have evolved since 1984, it is better to refer this model as a terrorism counteraction model, because it encompasses both counterterrorism and antiterrorism measures. The seven-step model was developed by US Army Military Police and Special Forces personnel as a planning model of the 1980's to guide the protection of US facilities and personnel. Much of the focus of the original model was on prevention and mitigation, so there is no easy way to empirically measure its effectiveness because there is no method to accurately measure acts of terrorism that were deterred or prevented. However, this counteraction model is useful to us as a starting point from which we can plan for response to biological terrorism.

Figure [see attached]

An 8 Step Model adapted to the Medical Community: It is difficult to develop a planning template for biological terrorism scenarios, given that there is little history of bioterrorism from which to derive lessons. There has been only one significant successfully executed act of biological terrorism in the United States[2]. However, the static seven-step model described above can be adapted to the medical community. Bringing the model forward from 1984 to 2000, it becomes a dynamic eight-step model (see figure 3):

Step 1 — Medical Intelligence — Intelligence is the collection, evaluation, and dissemination of information. In a military or law enforcement milieu, intelligence collection is the use of various methods to collect information on an adversary or the operating environment. Intelligence professionals categorize intelligence according to the mode of collection: human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT), for example. Much of what law enforcement and military officials call intelligence is of little relevance to the medical provider. However, as part of preparedness for a biological terrorism incident, medical intelligence will primarily be the responsibility of public health officials and epidemiologists.

Medical Surveillance — Public health surveillance is "the ongoing, systematic collection, analysis, interpretation, and dissemination of health data,"[3] with the intent of providing indications and warning. Using this definition, public health surveillance is an intelligence discipline. There are a number of potential epidemiological features of potential biological agents. The following epidemiological indicators are widely respected and should provide intelligence indications:

- Rapidly increasing morbidity (within hours or days) in a normally healthy population.
- An epidemic curve that rises and falls sharply during a short period of time. With contagious agents, successive peaks may occur.
- A sharp increase in the number of patients presenting with similar fever, respiratory, or gastrointestinal complaints.
- An endemic disease emerging at an uncharacteristic time, unusual geographic location, or in an unusual pattern.
- Unusual or unseasonal presence of vector animals (arthropods or rodents).
- Unexplained deaths or illnesses among livestock or wild animals.
- Clusters of patients arriving from a single locale. This could be an indicator of a point source biological attack.
- Large numbers of rapidly fatal cases.
- Lower morbidity among people who have been indoors, especially in areas with filtered air or closed ventilation systems, compared with people who have been outdoors. (Or the converse case.)

- Patients presenting with uncommon diseases that have bioterrorism potential, such as pulmonary anthrax, glanders, tularemia, or pneumonic plague. [4]

Centers for Disease Control programs such as the Epidemiology and Laboratory Capacity (ELC) program, and the Emerging Infections Programs (EIP) provide useful capabilities in this regard. However, the front line is the medical provider, the "provider based sentinel network."[5] Surveillance is critical to the control of biological incidents. Bolstering surveillance efforts will be required to deal with emerging biological agent threats. True early warning, in the military intelligence sense is unlikely; intelligence will be gained from clusters of diagnosed cases. The clinician will provide initial warning.

Medical Intelligence — Agent Identification: Rapid detection and identification of biological weapons is problematic. The clinician will provide initial warning. Detection will be diagnosis. Laboratory procedures have evolved much more than field techniques. Aside from some sporadically available immunochromatographic assay tickets, the medical community still must rely on laboratory methods. Various techniques are useful:

- Culturing and isolating a pathogen
- Animal inoculation
- Mass spectroscopy (for toxins)
- Detection of antibodies (specific immunoglobulins)
- Immunoassay detection of antigens
- DNA probes
- Detection of a pathogen's metabolic products in clinical specimens[6]

Step 2 - Threat Analysis — Threat analysis is a continuous process of assessment of specific threats, awareness of threat capabilities, forecasting future vulnerabilities, and identification of weaknesses. The planner must expend significant effort in this step. It is important to note that this model is not strictly a chronological or static model; it is a template for a deliberate and dynamic thought process. Therefore, intelligence does not cease to be collected while threat analysis occurs.

Agent Awareness: Medical providers should achieve a reasonable level of knowledge of the biological warfare threat and biological terrorism. It is incumbent upon the medical care system to have basic knowledge of the technical characteristics (signs and symptoms, laboratory indications, transmissibility, course of treatment, etc.) of pathogens or toxins of terrorist significance.

Identification of New Potential Threats: Any biological warfare agent has characteristics that make it useful as a weapon. A number of characteristics are widely held to be useful for a pathogen or toxin to have terrorist utility:

- Ease of production
- Lethality or incapacitation in a reasonable dose
- Particle size distribution in aerosol ideal for inhalation
- Ease of dissemination
- Stability in storage
- Susceptibility of target
- Non-susceptibility of friendly forces

Threat Analysis: Forecasting Vulnerability and Identifying Weakness: The planner must expend effort to analyze existing plans, personnel, and infrastructure for vulnerability to biological terrorism scenarios. This is far more than mere susceptibility to the actual threat pathogen or toxin. Rather, it is an analysis of systemic weaknesses as well as specific shortcomings. Medical providers, especially those tasked with development of disaster plans, will need to work closely with other community planners, including state and local emergency management agencies and law enforcement agencies to understand vulnerabilities. Naturally, these agencies will vary according to the particular locality.

Threat Analysis - Credibility Assessment: The most accurate and timely intelligence in the world is useless if it not used properly. There are several ways in which threat analysis is useful for medical providers. Perhaps one of the most important roles that medical providers can play in combating biological threats is credibility assessment. The employment of biological agents provides tremendous hoax potential. Knowledgeable medical providers can prove to be a valuable resource in hoax assessment and defuse the drama associated with biological threats. They can work directly with law enforcement agencies, including negotiators, if a specific threat has been announced. Likewise, medical authorities can work as consultants to the media to ensure that accurate information is released, not hysteria or hyperbole.

A basic approach to biological hoax assessment should assess a threat from three separate perspectives:

- Scientific: Does the purported threat have technical validity? Does the purported biological agent have the characteristics to achieve the perpetrator's goals?
- Operational: Is the threat realistic from an operational or logistical standpoint?
- Psychological: Has the perpetrator or group displayed any psychological traits that indicate his/her willingness to execute the threat?

Ideally, an assessment team could be set up to assess a hoax, with experts divided into separate scientific, operational, and psychological assessment cells. Infectious disease experts and microbiologists could perform the scientific assessment. Law enforcement and military experts could provide valuable insight in an operational cell. Psychologists and psychiatrists will have to participate in the psychological assessment cell.

Conversely, poorly informed medical authorities can play into the hands of hoax perpetrators and exacerbate the situation. It is quite possible that a well-intentioned but misinformed physician may lend credibility to an otherwise harmless threat. It is paramount that medical providers obtain and maintain a reasonable level of education and know when and where to receive additional information.

Steps 3 to 6 - Defensive Measures — Antiterrorism: In this bioterrorism counteraction model, the collection and analysis of threat information drives the development and implementation of protective measures designed to deter attack or, more likely, mitigate the results of a biological attack. This is antiterrorism — measures taken to increase defense against terrorist attack. The military and law enforcement model of antiterrorism includes several security disciplines—physical security, personal security, and operational security. Collectively, these disciplines are often referred to as force protection in a military context today. These defensive disciplines are readily adaptable for civil use. The results of the threat analysis process will highlight the required defensive measures.

Step 3 - Physical Security: Borrowing once again from the military and law enforcement model, physical security comprises those measures taken to provide protection to facilities and physical infrastructure. Some physical security considerations appropriate to the medical community include:

- Hospital Security / Crowd Control — Civil disorder may become a distinct problem in the event of a widespread biological incident. Walking wounded and - more importantly — walking worried can easily overwhelm hospital emergency departments. Liaison should be made with local and state law enforcement agencies, to include the National Guard to ensure that security augmentation can be made available for contingency scenarios.
- Decontamination: Depending on the biological agent employed, prompt and efficient decontamination is important to limit the spread or transfer of contamination. It is unlikely that decontamination will be a concern in biological terrorism scenarios, given that patients will present well after actual exposure to the agents. The large majority of biological warfare agents are not persistent.[7] Agents in spore form (such as Anthrax) and many toxins may require decontamination.
- Physical Infrastructure: Architecture and engineering can be used to mitigate the effects of biological terrorism, much like the mitigation of conventional explosive hazards. Security of air intakes is particularly important. Closed spaces greatly facilitate the efficiency of biological weapons. Most of the clinical cases of pulmonary anthrax (wool-sorter's disease) in the twentieth century were due to exposure in closed spaces.[8]

Step 4 - Personal Security: Common-sense measures, to include and expand upon universal precautions, should be taken to mitigate the hazards potentially faced by medical personnel. Furthermore, biological agents that pose a threat of contagion may be spread using medical providers as a vector, turning hospitals into hot zones. (Ebola outbreaks in Zaire demonstrated this phenomenon.) It is incumbent upon hospitals and public health officials that they insure protection of medical personnel.

- Protective Equipment: The use of personal protective equipment must be considered. Universal precautions (BL-2) are a useful starting point until the agent is identified. Although less important than in chemical scenarios, protective clothing is an important planning consideration.
- Immunization: Ideally, vaccination is the preferred defensive tactic. In most scenarios, however, immunization is probably not a useful option for protection of medical personnel due to the timelines involved. However, in other scenarios, immunization may be critical to ensuring the safety of responders. This is clearly the case with smallpox.
- Chemoprophylaxis: If the threat is or is suspected to be bacteria or rickettsia, chemoprophylaxis may be the best option to protect personnel. Chemoprophylaxis is more limited when viruses are the threat.

Step 5 - Defensive Measures- Operational Security: Physical security is the protection of the integrity of physical infrastructure and personal security is the protection of individual personnel. Operational security is the protection of the overall integrity of the health system. In a wide-spread casualty situation, mortality equals prevalence times seriousness, divided by access to health care.[9] Conventional-type attacks on various aspects of the health system can act as force multipliers for a biological attack. In the bioterrorism setting, operational security can easily include the following:

- Situational Awareness: It is important for planners and responders to build and maintain good lines of communication, both horizontally (between providers at the same echelon) and vertically (from EMS to hospitals to public health to federal experts).
- Vector Control: Certain biological agents may be disseminated through vectors. Vector control clearly ties in with medical intelligence collection. Poor medical intelligence could lead to eradication of the wrong vector (i.e., killing the rats instead of the fleas, who merely find a new home).
- Safety of Water supplies: Drinking water is safer than some critics might imagine. However, vulnerabilities do exist. In 1993, Milwaukee faced a massive outbreak of watery diarrhea caused by cryptosporidium cysts that passed through the filtration system of one of the city s water treatment plants. Water-quality standards and the testing of patients for cryptosporidium were not adequate to detect this outbreak.[10]
- Transportation: Patients, support staff, pharmaceuticals, medical equipment, and medical experts have to move from point to point. In a crisis situation, National Guard assets (both Army and Air Force) may prove useful. Medical providers should request assistance through their state National Guard's Military Support to Civil Authority office.

- Supply Chain Security: Medical care is logistically vulnerable. Every hospital and clinic requires resupply of consumable materiel. The surety of the supply chain is important to operational security.

Step 6 — Defensive Measures — Information Security: In the 1984 Army terrorism counteraction model, information security was addressed as a sub-discipline of operational security. However, in the information age, the safety and integrity of information and information systems deserves to be identified as a distinct security discipline and defined as a separate step in the response model. The ubiquitous automation of hospitals and medical information increases vulnerability to cyberterrorism and information warfare. Information warfare can multiply the effects of a biological attack by contributing greatly to the chaos. Comparatively little effort has been exerted in overlaying the information warfare and biological terrorism threats, nor has much effort been made to understand the overall vulnerability of the medical infrastructure to electronic attack. (See scenario below.) It is important for each medical provider to understand his or her own reliance on automation. Information security should examine all of the following:

- Surveillance: Epidemiological tracking is increasingly reliant upon computerization and telecommunications.
- Patient Records: Patient records are becoming more automated than in the past. Destruction or corruption of computerized patient records will hinder effective care.
- Horizontal Communications: Communications between hospitals and between doctors is vulnerable to attack. Interdicted communications will hinder a coordinated response.
- Vertical Communications: Likewise, communications between local hospitals and public health authorities and the various national-level assets (USAMRIID, CDC, etc.) are vulnerable to interdiction.
- Technical Reference: Physicians rely upon an increasingly diffuse body of knowledge to help them diagnose and treat patients. Standard printed reference texts are often obsolete within a few years of publication. The internet is used extensively for rapid research on diagnosis and treatment, especially for rare or exotic conditions. The large variety of electronic resources available to physicians is highly vulnerable to attack and could be tainted with disinformation.
- Clinical Diagnostics: Modern hospital laboratories make extensive use of computerization. Damage to hardware or software will hinder many laboratory procedures that may be necessary for diagnosis and treatment.
- Power Grids: Commercial power to hospitals may be endangered.

Step *7* - Authority and Jurisdiction: In the military and law enforcement model, authority and jurisdiction are largely legal issues, heavily involved with the investigation and prosecution of criminal acts. As such, authority and jurisdiction issues can easily be overlooked by medical providers and health authorities, given that their primary concern is public health and safety, not investigation and prosecution. Authority and jurisdiction, though, is important in the context of isolation and quarantine. The original seven-step model of the 1980's left this step unconnected with the other steps in that static model. However, it should be considered a planning consideration for step 8.

Quarantine authority: Quarantine is the application of control measures to individuals or modes of transport to prevent the spread of disease.[11] Quarantine is a breach of individual freedom and is difficult to reconcile with the nature of a free and democratic nation. It is a complicated legal issue. In general, quarantine measures are unlikely to be needed with most biological warfare agents. Pneumonic plague and Smallpox are the likely exceptions. A single individual

Information Warfare and Biological Terrorism:

County General Hospital relies heavily on its new computerized system for management of patient records, scheduling of staff, reporting laboratory results, and many other management functions. County General is the largest hospital in its region and is the primary ED in its municipality. A large, Fortune 500 computer company is headquartered nearby.

On October 1, the corporate headquarters was the target of a biological terrorist attack. Bottled drinking water was contaminated with Salmonella typhimurium. Throughout the next day and into the next week, dozens of patients arrive at County General seeking treatment for acute gastroenteritis. However, the hospital's response to this incident is severely hindered. Several computer viruses deliberately planted at County General have caused the following:

- The computerized staff scheduler program has scheduled fewer personnel than normal for duty that week.
- Pharmaceutical inventories are in disarray.
- Lab results for many patients are corrupted, showing false critical laboratory values. Stool cultures are improperly logged in the lab's computer system.
- Patient records are corrupted. Antibiotic allergies are omitted or altered in patient s charts and in the pharmacy.
- The telephone system is compromised. Internal phone calls are routed to the wrong extension. Calls to pathology are routed to pediatrics; calls to nephrology are routed to personnel. Persons placing calls to the hospital receive busy signals. Outgoing calls are difficult to make, hindering recall of staff and con tact with outside authorities.
- The local poison control center's technical databases have been corrupted with false information.
- The county's EMS dispatch system is hindered, causing all Salmonella patients to be transported to County General instead of bypassing it and dispersing the patients elsewhere.

exposed to smallpox in 1963 traveled by air from Australia to Sweden. He made intermediate stops in Djakarta, Singapore, Rangoon, Calcutta, Karachi, Teheran, Damascus, and Zurich. At least 19 cases of smallpox resulted from exposure to the affected individual. (300,000 people were vaccinated, however.[12])

Quarantine authority is diffuse at the federal level. It is constitutionally constrained to controlling passage into or out of the United States or between states.[13] Federal quarantine authority is further constrained to those diseases specified by Executive Order 12452: cholera, diphtheria, infectious tuberculosis, plague, smallpox, yellow fever, and viral hemorrhagic Fevers.[14] Quarantine is primarily a state and/or local responsibility. The authors have made no attempt to summarize quarantine regulations throughout the US, but it is incumbent upon planners and responders to understand the laws and regulations in their local areas.

Laws and Treaties: A variety of laws and treaties have bearing on authority and jurisdiction in the case of biological terrorism. Various pieces of US legislation include the Weapons of Mass Destruction statute (18 USC 2332a), the Biological Weapons Antiterrorism Act (18 USC 175), the dangerous devices statute (18 USC 921) and food tampering laws. Constitutionally, treaties ratified by the United States are also considered law, although most also have laws enacted to implement them. Such treaties as the Geneva Convention (1929) and the Biological and Toxin Weapons Convention (1975) provide a basic international framework for nonproliferation and counterproliferation. A basic understanding of the law is important, given that the medical community will have to work closely with the law enforcement community. The law enforcement community will use the existing laws to arrest and prosecute perpetrators. Clinical specimens may be needed as evidence. A laboratory match between S. typhimurium samples taken from a terrorist's lab and samples from patients was a key piece of intelligence and evidence in the 1983 Oregon case.[15]

Step 8a Crisis/Consequence Management - Planning: The planner and responder must bring together all of the considerations raised in steps one through seven and put them together in this step of the model. If developing plans from scratch, this is the step in which all of the information gained in the other steps is put to use. Often, existing disaster plans may provide a useful point of departure. If refining your planning due to a specific incident or threat, then the existing plans must be reviewed and updated as needed. It is critically important to establish dialogue and interagency communications, both horizontally and vertically, well before the advent of any crisis. History has demonstrated that communication usually degrades in time of crisis. Communications that are poor or non-existent will not improve during an incident; inadequate links will not become good.

The development of specific plans for biological terrorism is a science still in its infancy. While not necessarily definitive, a good example of how to start is the guidance promulgated by the Maryland Institute for Emergency Medical Services System (MIEMSS) in April 2000. Their 20-point guidance for hospitals seems thorough and suggests a hospital's plan include the following components:

1.) Establishment of alternate treatment centers both on and off hospital campuses;
2.) Arrangements for sheltering occupants, staff, patients, and visitors from the elements;
3.) Arrangements for decontamination of staff, patients, and visitors;

4.) Arrangements for inter-facility and inter-hospital credentialing of medical staff and other personnel to allow for lateral utilization of human resources;
5.) Credentialing of volunteers not affiliated with a health-care facility;
6.) Arrangements for back-up, reserve, and back-fill for medical equipment and supplies;
7.) Arrangements for security for facilities and any alternate sites;
8.) Patient identification and tracking systems;
9.) Adequacy of potable water, food, and sanitary waste disposal;
10.) Arrangements for establishing temporary morgues;
11.) Procedures and treatment protocols for separating and handling victims, casualties, and the worried well;
12.) Arrangements for psychiatric and counseling services for incoming patients or persons who require assistance;
13.) Arrangements for shift rotations and extended duty hours;
14.) Arrangements for Critical Incident Stress Management for health-care personnel;
15.) Protocols for discontinuing services at or by a facility;
16.) Arrangements for financial accounting for costs incurred by the response;
17.) Arrangements for mutual assistance and aid by other facilities or hospitals;
18.) Arrangements for an integrated unified command system;
19.) Arrangements for a coordinated Public Information Office in conjunction with state emergency management official;
20.) Arrangements for any locally identified issues that would be of concern or a problem for the local community.[16]

In general, medical plans should cover surveillance and early detection, health and medical resource coordination, mass patient care, mass fatality management, environmental health, and public information/education.

Crisis/Consequence Management - Performing: Once an event occurs, there is no longer any time for planning. The medical community must act based on the information and analysis from steps one through seven. Existing plans must be enacted. It is important that the medical community work in conjunction with other responders, such as law enforcement, fire/EMS, federal agencies, emergency management agencies, and others. Efforts by health care providers will happen within a broader context. Health care is important both in crisis management and consequence management. A unified, multidisciplinary, and proactive approach is needed. Incident Command System (ICS) principles, used by first responders, can be incorporated. Figure 2 provides a conceptual framework for incident management.

Figure 2: Incident Management Structure

Refining the model — Making the model dynamic.

The 1984 counterterrorism model was a static model best suited for planning for a single incident for protecting a single person or facility. We have turned the 1984 7-step model into an 8-step bioterrorism response model (see figure 3). Rather than a specific road map, it is a logical and continuous thought process. Earlier steps of the model can and should be modified as needed; shortcomings will be evident when plans are written. Furthermore, the entire model can be adjusted based on the results of actual incident response.

Future Threats: The future of the biological threat is as speculative as its present. Like any other type of potential terrorist weapon, there is not necessarily any reason for terrorists of any flavor or type to restrict themselves from employment of biological agents. It is also important to note that employment of biological weapons and an act of biological terrorism are legally the same thing under current laws (BW Antiterrorism Act). However, this muddles the classical definition of terrorism. Not every conceivable scenario for employment of biological agents is performed by those motivated by the traditional ideological or religious motives for acts of terrorism. Since pathogens and toxins have utility as weapons, it is altogether possible that individuals or groups without "traditional" terrorist motivations may employ them for non-political, non-ideological, and non-religious reasons. Alliances between terrorist groups and organized criminal activity, (e.g., the Chechen underworld in the former Soviet Union) are increasingly common. Stricter criminal statutes in penal codes around the world covering "hate crimes" and various flavors of "terrorism" blur the distinction between criminal violence and terrorism. The trial and conviction of Theodore Kaczynski further obfuscates the issue by reducing distinctions between terrorism and insanity. Organized crime, "narco-terrorists," and lone individuals are likely to be the next important wave of the biological threat. However, neither the technical characteristics of biological agents nor the neuropsychiatric aspects of the perpetrators matter that much if proper planning is not undertaken well in advance of an incident. Chaos among the responders is a force multiplier for the attacker.

Figure [see attached]

Summary and Conclusion: In closing we have more concern with the psychology of terrorism than with its microbiology. The future of "the Threat" is the neurochemistry of the "agents" of the new groups and the new coordination of terrorist groups. The neurochemistry we refer to is the behavior of those who choose NBC instead of incinerator or explosive devices. A concise statement by Director of Central Intelligence George Tenet before the Senate Armed Services Committee Hearing on Current and Projected National Security Threats (2 February, 1999) mirrors our concerns. Mr. Tenet states that his concern for those organizations who feel that the acquisition of CBRN weapons is "a religious duty" and that his greatest concern is that "the potential profitability of smuggling items related to WMD may lead to organized criminal involvement in brokering deals, financing transactions, or facilitating the transport of WMD materials to rogue states and terrorist groups." Although the dynamics of terrorism continue to change, the threat to infrastructure is still a short-term goal of terrorism. Our paper is designed to build infrastructure by building upon the communication system between law enforcement and the medical community.

---

[1] US Department of Justice and Federal Emergency Management Agency, "Emergency Response to Terrorism Self Study Course," June 1999.

[2] JAMA, 6 Aug 1997, Vol 278, No. 5, pp 389-395.

[3] National Center for Infectious Diseases, Centers for Disease Control and Prevention, October 21, 1996.

[4] Pavlin, Julie A., "Epidemiology of Bioterrorism," *Emerging Infection Diseases,* July-August 1999.

[5] NCID/CDC, *op cit.*

[6] US Army CHPPM Tech Guide 244: *The Medical NBC Battlebook*, US Army Center for Health Promotion and Preventive Medicine (CHPPM), 1999. p. 4-17.

[7] JAMA, 3 May 2000 Vol. 283 No17.

[8] Ann NY Acad Sci 1980;353: pp. 83-93. See also Am J Med. 1960; pp. 29:992-1001.

[9] International Committee of the Red Cross; *War and Public Health*, 1996.

[10] New England Journal of Medicine, 1994; 331 : pp. 161-167.

[11] Centers for Disease Control and Prevention, *Health Information for International Travel —1995*, Aug. 1995, p. 194.

[12] Domestic Preparedness Training Program, Defense Against Weapons of Mass Destruction, Technician-Hospital Provider Course, 1998.

[13] 42 United States Code 264.

[14] Executive Order 12452, Dec 22, 1983.

[15] JAMA, 6 Aug 1997, *op. cit.*

[16] Maryland Health and Medical System Preparedness Response Plan — Weapons of Mass Destruction, April, 2000, 46-47.

Bio-Medical Aspects of Bio-Terrorism and a Call to Action

Paul B. Roth, M.D., Brian Hjelle, M.D., and John K Gaffney, BBA, CEM, TEMT-P

Not since the height of the cold war has there been so much public concern over weapons of mass destruction. Many of the current fears focus on the threat of the intentional release of infectious agents. The nightmare image of tens of thousands of bodies lining the streets of American cities accompanies these concerns. Such fears have been fueled by both popular fiction and actual accounts of deliberate exposures throughout the world. The use of biological agents can be even more dangerous than nuclear weapons since a nuclear attack has a limited area of effect, albeit huge, and it is obvious when there is a nuclear explosion. Technology to detect and quantitate radioactive contamination is very widely available. In comparison to nuclear attacks, some biothreat agents can initially spread silently and unchecked through populations far from ground zero **.**

Biological agents have been considered for use as weapons on unsuspecting populations throughout history. Recent examples are the use of Yersinia *pestis*-infected fleas by the Japanese on the Chinese during World War II, and more recently the threat of *Bacillus anthracis* use in the Gulf War. In most cases, the results of the use of these kinds of weapons have been less than impressive in comparison to those obtained with more conventional weapons. What, then, has changed to make bio-terrorism more of an issue than in the past?

One answer is the psychological impact of this type of threat. The public is much more aware of new emerging pathogens. Gruesome photographs of bloodied bodies in Africa after exposure to the Ebola virus were widely distributed. The unseen, and in all other respects, undetected attack which could result in the images described above make for a very effective terrorism weapon in and of itself.

Another change which causes even the most conservative among us to be alarmed involves the incredible advances in biotechnology. It is now possible to alter the most virulent bacterium or virus and make it both more pathogenic and less likely to be killed by conventional therapy. The molecular biology revolution has now been underway for more than three decades, and the sheer number of persons with dangerous technical expertise has increased exponentially since the 1960s.

Finally, our populations are routinely engaged in global activities, traveling easily and often to distant locations. The likelihood of rapid dissemination of any type of biological agent worldwide in a very short period of time is high, and the general public is well aware of this fact.

The challenges facing our ability to effectively defend against bio-terrorism are much greater today. In part, this is because of the ease in which high density population centers within the United States and elsewhere may be exposed to these agents. Further, infected individuals will spread these genetically altered organisms — with their high rate of mortality and/or morbidity - with great rapidity. Additionally, the current efforts to develop these defenses are uncoordinated and lacking vision. There are hundreds of millions of dollars that have been identified to address a number of aspects of this defense but there does not appear to be a well defined strategic plan directing these efforts.

While the scientific community is actively engaged in developing methods of early detection and customized, rapid treatment strategies (vaccines, anti-virals and/or other drug therapies), there is no national approach to coordinate these efforts. This must also be done in conjunction with other responses, including interdiction of additional attacks, containment of exposure and treatment of those infected. Finally, the majority of funds for responding to a bio-terrorism event are currently given to the federal response community. This must be shifted so that training and equipping of first responders (and health care providers) must be funded, planned and then implemented at the local level, where any initial response to a Weapon of Mass destruction (WMD) event will be.

A successful approach to overcome these challenges must include collaborative programs between federal and state governments, the private sector and academic institutions. When facing the threat of national security during World War II, the Manhattan Project was designed in this fashion with incredible results. The problems described above that are associated with bio-terrorism pose a level of complexity many orders beyond those of simply developing an atomic weapon.

In an effort to better understand and create effective interventions against bio-threats the University of New Mexico School of Medicine has formed a coalition with Los Alamos National Laboratories (LANL), Sandia National Laboratories, the New Mexico State Department of Health and Lovelace Respiratory Research Institute. Among the first projects of this Consortium is the development of a model for population surveillance utilizing real-time reporting by health professionals in an emergency department of all patients with presenting complaints consistent with a flu-like illness. This model system expands and builds on existing systems of detection by employing network-based reporting through internet connectivity and simple computer screen displays for entering syndrome-based reports by touch screen entry.

Although starting in a single emergency department, the intent is to quickly extend this system to public health offices and other major health centers throughout the state of New Mexico. The purpose of this initial project is to demonstrate the ability of the national labs, private industry and an academic health center to work cooperatively to address a common problem. Specifically, the project will develop an efficient model for rapidly detecting new clusters of infections in a population, and to develop the informational tools and datasets that will lead us to the ability to distinguish natural from manmade outbreaks. The model could yield immediate practical benefits such as the identification of early outbreaks of naturally occurring illnesses caused by influenza, enteroviruses, or the respiratory syncytial virus.

There are a number of other, more fully developed pilot projects underway involving members of the Consortium. UNM School of Medicine faculty and scientists from Sandia

National Laboratories and LANL are working on several pilot projects to develop ultrasensitive biosensors for directly detecting pathogenic viruses in the environment, as well as a project that uses near-infrared spectroscopy to detect changes in cells that may mimic the changes that occur very early in the infection of an animal. The School of Medicine s Infectious Diseases and Inflammation Program (IDIP) is using the Consortium s expertise to train a new generation of basic scientists whose highly interdisciplinary, broad-based training in infectious diseases and immunology will equip them to lead future efforts. The IDIP program has been awarded an NIH T32 training grant to support the development of students trained to use the latest technologies to address infectious disease threats both natural and manmade.

Future projects in the planning stages include: rapid detection and genomic analysis of suspected biological threats; bioinformatics tools for pattern recognition of unusual events; and tools for rapidly identifying the appropriate intervention and response. Detection of pathogens by using conventional markers for infection such as specific antibodies, nucleic acids or propagation in culture is intrinsically very slow and will not be suitable for many types of biological attacks, especially with engineered agents. However, investigators at UNM s IDIP are developing novel tools to examine host responses to infection with the goal of categorizing infectious processes into groups based upon host responses. It is their hypotheses that identification of common molecular pathways of host responses by specific agents will enable them to examine the agent s pathological footprint - long before conventional specific tests become positive. Thus anthrax may be clustered together with another bacterial process and enable investigators to make the immediate step toward therapies that interfere with the harmful host response while simultaneously adding antimicrobials that treat all of the candidate agents, which were previously assigned a similar footprint .

An additional important role for this Consortium will include training of physicians and first responders as well as young scientists in the fields of toxicology and infectious disease through the School of Medicine s Center for Disaster Medicine (CDM). The CDM not only provides the educational expertise to accomplish this training, but also fields the nation s largest disaster medical team, thus providing a test bed for hardware, software, and procedures developed by the Consortium. It will thus provide a mechanism for translating the knowledge developed in the laboratory into the practical application of this knowledge in the field during actual releases of bio-terrorism agents.

Barriers to successfully achieving these local consortium goals are the inherent bureaucracies of our respective institutions on one hand and the lack of access to special facilities, specifically Bio-Safety Level 4 (BSL-4) labs. These laboratories are designed to allow scientists to safely study the lethal organisms that bioweaponeers are most likely to release. Currently, these high-containment labs are located in only a few areas in the country with only limited access by the general scientific community. At this time, there are only four of these laboratories located in this country (NIH, Bethesda, Maryland; CDC, Atlanta, Georgia; US Army Medical Research Institute of Infectious Disease, Fort Detrick, Maryland and Southwest Foundation for Biomedical Research, San Antonio, Texas). Prior to two years ago there were only two Level 4 labs, and they were for the most part restricted to government use. Although there are four more labs being planned (three in Texas and one on Plum Island, New York) access and therefore scientific discovery will still be limited. Even if all of those planned facilities are built, the US will still be markedly lacking in the high-throughput vaccine and therapeutic testing capability that is demanded to meet the threat of bioweapon attack.

The current threat of a deliberate release of highly contagious and virulent micro-organisms by individuals who intend to terrorize the American public is a very real one. It is therefore imperative for federal, state and local governments to forge effective alliances with the public and private scientific communities in mounting a meaningful mitigation and response strategy. This plan should include several critical aspects. First, further research in the fields of microsystems for the development and wide distribution of devices for the early detection of selected organisms in the environment. Second, continued research in bio-medical sciences in an effort to rapidly recognize individuals who are infected with bio-threat organisms and in the development of customized therapies. Third, to slow and eventually halt the spread of these bio-terrorism agents there must be rapid containment strategies and facilities. And finally, mass training of first responders and health care providers who may be called upon to deal with these types of situations in local communities must be developed and implemented.

Given the aforementioned lack of coordination and unified leadership in the bio-terrorism community, there should be a special blue-ribbon panel created. It should be composed of federal, state and local government representatives, members of the scientific community (private sector, national laboratories and universities) and private industry. This panel should be charged with identifying a unified strategy to defend the American people against this immanent threat. Thereafter, a similarly unified structure must be developed and empowered to implement this strategy.

Terrorism Incident Annex[1]

Signatory Agencies: Department of Defense
Department of Energy
Department of Health and Human Services
Department of Justice
Federal Bureau of Investigation
Environmental Protection Agency
Federal Emergency Management Agency

I. Introduction

Presidential Decision Directive 39 (PDD-39), U.S. Policy on Counterterrorism, establishes policy to reduce the Nation s vulnerability to terrorism, deter and respond to terrorism, and strengthen capabilities to detect, prevent, defeat, and manage the consequences of terrorist use of weapons of mass destruction (WMD). PDD-39 states that the United States will have the ability to respond rapidly and decisively to terrorism directed against Americans wherever it occurs, arrest or defeat the perpetrators using all appropriate instruments against the sponsoring organizations and governments, and provide recovery relief to victims, as permitted by law.

Responding to terrorism involves instruments that provide crisis management and consequence management. "Crisis management" refers to measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The Federal Government exercises primary authority to prevent, preempt, and terminate threats or acts of terrorism and to apprehend and prosecute the perpetrators; State and local governments provide assistance as required. Crisis management is predominantly a law enforcement response. "Consequence management" refers to measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise primary authority to respond to the consequences of terrorism; the Federal Government provides assistance as required. Consequence management is generally a multifunction response coordinated by emergency management.

Based on the situation, a Federal crisis management response may be supported by technical operations, and by Federal consequence management, which may operate concurrently (see Figure TI-1). "Technical operations" include actions to identify, assess, dismantle, transfer, dispose of, or decontaminate personnel and property exposed to explosive ordnance or WMD.

1. Federal Emergency Management Agency (FEMA): Incident Annexes to the Federal Response Plan, April 1999, http://www.fema.gov/r-n-r/frp/frpterr.htm

Source: HHS/FEMA

Figure TI-1 Relationship Between Crisis Management and Consequence Management
[Figure: SEE ATTACHED]

A. Purpose

The purpose of this annex is to ensure that the Federal Response Plan (FRP) is adequate to respond to the consequences of terrorism within the United States, including terrorism involving WMD. This annex:

1. Describes crisis management. Guidance is provided in other Federal emergency operations plans;

2. Defines the policies and structures to coordinate crisis management with consquence management; and

3. Defines consequence management, which uses the FRP process and structure, supple-mented as necessary by resources normally activated through other Federal emergency operations plans.

B. Scope

This annex:

1. Applies to all threats or acts of terrorism within the United States that the White House determines require a response under the FRP;

2. Applies to all Federal departments and agencies that may be directed to respond to the consequences of a threat or act of terrorism within the United States; and

3. Builds upon the process and structure of the FRP by addressing unique policies, situa tions, operating concepts, responsibilities, and funding guidelines required for response to the consequences of terrorism.

II. Policies

A. PDD-39 validates and reaffirms existing lead agency responsibilities for all facets of the U.S. counterterrorism effort.

B. The Department of Justice is designated as the lead agency for threats or acts of terror ism within U.S. territory. The Department of Justice assigns lead responsibility for opera tional response to the Federal Bureau of Investigation (FBI). Within that role, the FBI operates as the on-scene manager for the Federal Government. It is FBI policy that crisis management will involve only those Federal agencies requested by the FBI to provide expert guidance and/or assistance, as described in the PDD-39 Domestic Deployment Guidelines (classified) and the FBI WMD Incident Contingency Plan.

C. The Federal Emergency Management Agency (FEMA) is designated as the lead agency for consequence management within U.S. territory. FEMA retains authority and responsibility to act as the lead agency for consequence management throughout the Federal response. It is FEMA policy to use FRP structures to coordinate all Federal assis tance to State and local governments for consequence management.

D. To ensure that there is one overall Lead Federal Agency (LFA), PDD-39 directs FEMA to support the Department of Justice (as delegated to the FBI) until the Attorney General transfers the overall LFA role to FEMA. FEMA supports the overall LFA as permitted by law.

III. Situation

A. Conditions

1. FBI assessment of a potential or credible threat of terrorism within the United States may cause the FBI to direct other members of the law enforcement community and to coor dinate with other Federal agencies to implement a pre-release response.

a) FBI requirements for assistance from other Federal agencies will be coordinat ed through the Attorney General and the President, with coordination of National Security Council (NSC) groups as warranted.

b) FEMA will advise and assist the FBI and coordinate with the affected State and local emergency management authorities to identify potential consequence man agement requirements and with Federal consequence management agencies to increase readiness.

2. An act that occurs without warning and produces major consequences may cause FEMA to implement a post-release consequence management response under the FRP. FEMA will exercise its authorities and provide concurrent support to the FBI as appropri ate to the specific incident.

B. Planning Assumptions

1. No single agency at the local, State, Federal, or private-sector level possesses the authority and expertise to act unilaterally on many difficult issues that may arise in response to a threat or act of terrorism, particularly if WMD are involved.

2. An act of terrorism, particularly an act directed against a large population center with

in the United States involving WMD, may produce major consequences that would over whelm the capabilities of many local and State governments almost immediately.

3. Major consequences involving WMD may overwhelm existing Federal capabilities as well, particularly if multiple locations are affected.

4. Local, State, and Federal responders will define working perimeters that may overlap. Perimeters may be used to control access to the area, target public information messages, assign operational sectors among responding organizations, and assess potential effects on the population and the environment. Control of these perimeters may be enforced by dif ferent authorities, which will impede the overall response if adequate coordination is not established.

5. If appropriate personal protective equipment is not available, entry into a contaminat ed area (i.e., a hot zone) may be delayed until the material dissipates to levels that are safe for emergency response personnel. Responders should be prepared for secondary devices.

6. Operations may involve geographic areas in a single State or multiple States, involv ing responsible FBI Field Offices and Regional Offices as appropriate. The FBI and FEMA will establish coordination relationships as appropriate, based on the geographic areas involved.

7. Operations may involve geographic areas that spread across U.S. boundaries. The Department of State is responsible for coordination with foreign governments.

IV. Concept of Operations

A. Crisis Management
(Source: FBI, National Security Division, Domestic Terrorism/Counterterrorism Planning Section)

1. PDD-39 reaffirms the FBI s Federal lead responsibility for crisis management response to threats or acts of terrorism that take place within U.S. territory or in international waters and that do not involve the flag vessel of a foreign country. The FBI provides a graduated, flexible response to a range of incidents, including:

a) A credible threat, which may be presented in verbal, written, intelligence-based, or other form;

b) An act of terrorism that exceeds the local FBI field division s capability to resolve;

c) The confirmed presence of an explosive device or WMD capable of causing a significant destructive event, prior to actual injury or property loss;

d) The detonation of an explosive device, utilization of a WMD, or other destruc tive event, with or without warning, that results in limited injury or death; and

e) The detonation of an explosive device, utilization of a WMD, or other destruc tive event, with or without warning, that results in substantial injury or death.

2. The FBI notifies FEMA and other Federal agencies providing direct support to the FBI of a credible threat of terrorism. The FBI initiates a threat assessment process that involves close coordination with Federal agencies with technical expertise, in order to determine the viability of the threat from a technical as well as tactical and behavioral standpoints.

3. The FBI provides initial notification to law enforcement authorities within the affect ed State of a threat or occurrence that the FBI confirms as an act of terrorism.

4. If warranted, the FBI implements an FBI response and simultaneously advises the Attorney General, who notifies the President and NSC groups as warranted, that a Federal crisis management response is required. If authorized, the FBI activates multiagency cri sis management structures at FBI Headquarters, the responsible FBI Field Office, and the incident scene (see Figure TI-2). Federal agencies requested by the FBI, including FEMA, will deploy a representative(s) to the FBI Headquarters Strategic Information and Operations Center (SIOC) and take other actions as necessary and appropriate to support crisis management. (The FBI provides guidance on the crisis management response in the FBI WMD Incident Contingency Plan.)

Figure TI-2 Crisis Management Structures
[Figure: SEE ATTACHED FILE]

5. If the threat involves WMD, the FBI Director may recommend to the Attorney General, who notifies the President and NSC groups as warranted, to deploy a Domestic Emergency Support Team (DEST). The mission of the DEST is to provide expert advice and assistance to the FBI On-Scene Commander (OSC) related to the capabilities of the DEST agencies and to coordinate follow-on response assets. When a Joint Operations Center (JOC) is formed, DEST components merge into the JOC structure as appropriate. (The FBI provides guidance on the DEST in the PDD-39 Domestic Deployment Guidelines (classified).)

6. During crisis management, the FBI coordinates closely with local law enforcement authorities to provide a successful law enforcement resolution to the incident.

7. The FBI also coordinates with other Federal authorities, including FEMAThe FBI Field Office responsible for the incident site modifies its Command Post to function as a JOC and establishes a Joint Information Center (JIC). The JOC structure includes the follow ing standard groups: Command, Operations, Support, and Consequence Management. Representation within the JOC includes some Federal, State, and local agencies

(see Figure TI-3).

Figure TI-3 FBI Joint Operations Center Structure
[Figure: SEE ATTACHED FILE]

8. The JOC Command Group plays an important role in ensuring coordination of Federal crisis management and consequence management actions. Issues arising from the response that affect multiple agency authorities and responsibilities will be addressed by the FBI OSC and the other members of the JOC Command Group, who are all working in consultation with other local, State, and Federal representatives. While the FBI OSC retains authority to make Federal crisis management decisions at all times, operational decisions are made cooperatively to the greatest extent possible. The FBI OSC and the Senior FEMA Official at the JOC will provide, or obtain from higher authority, an imme diate resolution of conflicts in priorities for allocation of critical Federal resources (such as airlift or technical operations assets) between the crisis management and the conse quence management response.

9. A FEMA representative coordinates the actions of the JOC Consequence Management Group, expedites activation of a Federal consequence management response should it become necessary, and works with an FBI representative who serves as the liaison between the Consequence Management Group and the FBI OSC. The JOC Consequence Management Group monitors the crisis management response in order to advise on deci sions that may have implications for consequence management, and to provide continuity should a Federal consequence management response become necessary. Coordination will also be achieved through the exchange of operational reports on the incident. Because reports prepared by the FBI are "law enforcement sensitive," FEMA representatives with access to the reports will review them, according to standard procedure, in order to iden tify and forward information to Emergency Support Function (ESF) #5 Information and Planning that may affect operational priorities and action plans for consequence man agement.

B. Consequence Management

1. Pre-Release

a) FEMA receives initial notification from the FBI of a credible threat of terror ism. Based on the circumstances, FEMA Headquarters and the responsible FEMA region(s) may implement a standard procedure to alert involved FEMA officials and Federal agencies supporting consequence management.

b) FEMA deploys representatives with the DEST and deploys additional staff for the JOC, as required, in order to provide support to the FBI regarding consequence management. FEMA determines the appropriate agencies to staff the JOC

Consequence Management Group and advises the FBI. With FBI concurrence, FEMA notifies consequence management agencies to request that they deploy rep repsentatives to the JOC. Representatives may be requested for the JOC Command Group, the JOC Consequence Management Group, and the JIC.

c) When warranted, FEMA will consult immediately with the Governor s office and the White House in order to determine if Federal assistance is required and if FEMA is permitted to use authorities of the Robert T. Stafford Disaster Relief and Emergency Assistance Act to mission-assign Federal consequence management agencies to pre-deploy assets to lessen or avert the threat of a catastrophe. These actions will involve appropriate notification and coordination with the FBI, as the overall LFA.

d) FEMA Headquarters may activate an Emergency Support Team (EST) and may convene an executive-level meeting of the Catastrophic Disaster Response Group (CDRG). When FEMA activates the EST, FEMA will request FBI Headquarters to provide liaison. The responsible FEMA region(s) may activate a Regional Operations Center (ROC) and deploy a representative(s) to the affected State(s). When the responsible FEMA region(s) activates a ROC, the region(s) will notify the responsible FBI Field Office(s) to request a liaison.

2. Post-Release

a) If an incident involves a transition from joint (crisis/consequence) response to a threat of terrorism to joint response to an act of terrorism, then consequence man agement agencies providing advice and assistance at the JOC pre-release will reduce their presence at the JOC post-release as necessary to fulfill their conse quence management responsibilities. The Senior FEMA Official and staff will remain at the JOC until the FBI and FEMA agree that liaison is no longer required.

b) If an incident occurs without warning that produces major consequences and appears to be caused by an act of terrorism, then FEMA and the FBI will initiate consequence management and crisis management actions concurrently. FEMA will consult immediately with the Governor s office and the White House to deter mine if Federal assistance is required and if FEMA is permitted to use the author ities of the Stafford Act to mission-assign Federal agencies to support a conse quence management response. If the President directs FEMA to implement a Federal consequence management response, then FEMA will support the FBI as required and will lead a concurrent Federal consequence management response (see Figure TI-4).

c) The overall LFA (either the FBI or FEMA when the Attorney General trans fers the overall LFA role to FEMA) will establish a Joint Information Center in the field, under the operational control of the overall LFA s Public Information Officer, as the focal point for the coordination and provision of information to the public and media concerning the Federal response to the emergency. Throughout the response, agencies will continue to coordinate incident-related information through the JIC. FEMA and the FBI will ensure that appropriate spokespersons provide information concerning the crisis management and consequenct management responses. Before a JIC is activated, public affairs offices of responding Federal agencies will coordinate the release of information through the FBI SIOC.

Figure TI-4   Coordination Relationships
[Figure: SEE ATTACHED FILE]

d) During the consequence management response, the FBI provides liaison to either the ROC Director or the Federal Coordinating Officer (FCO) in the field, and a liaison to the EST Director at FEMA Headquarters. While the ROC Director or FCO retains authority to make Federal consequence management decisions at all times, operational decisions are made cooperatively to the greatest extent pos sible.

e) As described previously, resolution of conflicts between the crisis management and consequence management responses will be provided by the Senior FEMA Official and the FBI OSC at the JOC or, as necessary, will be obtained from high er authority. Operational reports will continue to be exchanged. The FBI liaisons will remain at the EST and the ROC or DFO until FEMA and the FBI agree that a liaison is no longer required.

3. Disengagement

a) If an act of terrorism does not occur, the consequence management response disengages when the FEMA Director, in consultation with the FBI Director, directs FEMA Headquarters and the responsible region(s) to issue a cancellation notifica tion by standard procedure to appropriate FEMA officials and FRP agencies. FRP agencies disengage according to standard procedure.

b) If an act of terrorism occurs that results in major consequences, each FRP com ponent (the EST, CDRG, ROC, and DFO if necessary) disengages at the appropri ate time according to standard procedure. Following FRP disengagement, opera tions by individual Federal agencies or by multiple Federal agencies under other Federal plans may continue, in order to support the affected State and local gov ernments with long-term hazard monitoring, environmental decontamination, and site restoration (cleanup).

V. Responsibilities

A. Department of Justice

PDD-39 validates and reaffirms existing lead agency responsibilities for all facets of the U.S. counterterrorism effort. The Department of Justice is designated as the overall LFA for threats of acts of terrorism that take place within the United States until the Attorney General transfers the overall LFA role to FEMA. The Department of Justice delegates this overall LFA role to the FBI for the operational response. On behalf of the Department of Justice, the FBI will:

1. Consult with and advise the White House, through the Attorney General, on policy matters concerning the overall response;

2. Designate and establish a JOC in the field;

3. Appoint an FBI OSC to manage and coordinate the Federal operational response (crisis management and consequence management). As necessary, the FBI OSC will convene and chair meetings of operational decision makers repre senting lead State and local crisis management agencies, FEMA, and lead State and local consequence management agencies in order to provide an initial assess ment of the situation, develop an action plan, monitor and update operational pri orities, and ensure that the overall response (crisis management and consequence management) is consistent with U.S. law and achieves the policy objectives out lined in PDD-39. The FBI and FEMA may involve supporting Federal agencies as necessary; and

4. Issue and track the status of actions assigned by the overall LFA.

B. Federal Bureau of Investigation

Under PDD-39, the FBI supports the overall LFA by operating as the lead agency for cri sis management. The FBI will:

1. Determine when a threat of an act of terrorism warrants consultation with the White House, through the Attorney General;

2. Advise the White House, through the Attorney General, when the FBI requires assistance for a Federal crisis management response, in accordance with the PDD-39 Domestic Deployment Guidelines;

3. Work with FEMA to establish and operate a JIC in the field as the focal point for information to the public and the media concerning the Federal response to the emergency;

4. Establish the primary Federal operations centers for the crisis management response in the field and Washington, DC;

5. Appoint an FBI OSC (or subordinate official) to manage and coordinate the cri sis management response. Within this role, the FBI OSC will convene meetings with operational decision makers representing Federal, State, and local law enforcement and technical support agencies, as appropriate, to formulate incident action plans, define priorities, review status, resolve conflicts, identify issues that require decisions from higher authorities, and evaluate the need for additional resources;

6. Issue and track the status of crisis management actions assigned by the FBI; and

7. Designate appropriate liaison and advisory personnel to support FEMA.

C. Federal Emergency Management Agency

Under PDD-39, FEMA supports the overall LFA by operating as the lead agency for con sequence management until the overall LFA role is transferred to FEMA. FEMA will:

1. Determine when consequences are "imminent" for the purposes of the Stafford Act;

2. Consult with the Governor s office and the White House to determine if a Federal consequence management response is required and if FEMA is directed to use Stafford Act authorities. This process will involve appropriate notification and coordination with the FBI, as the overall LFA;

3. Work with the FBI to establish and operate a JIC in the field as the focal point for information to the public and the media concerning the Federal response to the emergency;

4. Establish the primary Federal operations centers for consequence management in the field and Washington, DC;

5. Appoint a ROC Director or FCO to manage and coordinate the Federal conse quence management response in support of State and local governments. In coor dination with the FBI, the ROC Director or FCO will convene meetings with deci sion makers of Federal, State, and local emergency management and technical support agencies, as appropriate, to formulate incident action plans, define priori ties, review status, resolve conflicts, identify issues that require decisions from higher authori ties, and evaluate the need for additional resources;

6. Issue and track the status of consequence management actions assigned by

FEMA; and

7. Designate appropriate liaison and advisory personnel to support the FBI.

D. Federal Agencies Supporting Technical Operations

1. Department of Defense

As directed in PDD-39, the Department of Defense (DOD) will activate technical opera tions capabilities to support the Federal response to threats or acts of WMD terrorism. DOD will coordinate military operations within the United States with the appropriate civilian lead agency(ies) for technical operations.

2. Department of Energy

As directed in PDD-39, the Department of Energy (DOE) will activate technical opera tions capabilities to support the Federal response to threats or acts of WMD terrorism. In addition, the FBI has concluded formal agreements with potential LFAs of the Federal Radiological Emergency Response Plan (FRERP) that provide for interface, coordination, and technical assistance in support of the FBI s mission. If the FRERP is implemented concurrently with the FRP:

a) The Federal On-Scene Commander under the FRERP will coordinate the FRERP response with the FEMA official (either the ROC Director or the FCO), who is responsible under PDD-39 for coordination of all Federal support to State and local governments.

b) The FRERP response may include on-site management, radiological monitor ing and assessment, development of Federal protective action recommendations, and provision of information on the radiological response to the public, the White House, Members of Congress, and foreign governments. The LFA of the FRERP will serve as the primary Federal source of information regarding on-site radio log ical conditions and off-site radiological effects.

c) The LFA of the FRERP will issue taskings that draw upon funding from the responding FRERP agencies.

3. Department of Health and Human Services

As directed in PDD-39, the Department of Health and Human Services (HHS) will acti vate technical operations capabilities to support the Federal response to threats or acts of WMD terrorism. HHS may coordinate with individual agencies identified in the HHS Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological (C/B) Terrorism, to use the structure, relationships, and capabilities described in the HHS plan to support response operations. If the HHS plan is implement ed:

a) The HHS on-scene representative will coordinate, through the ESF #8 -— Health and Medical Services Leader, the HHS plan response with the FEMA official (either the ROC Director or the FCO), who is responsible under PDD-39 for on-scene coordination of all Federal support to State and local governments.

b) The HHS plan response may include threat assessment, consultation, agent identification, epidemiological investigation, hazard detection and reduction, decontamination, public health support, medical support, and pharmaceutical sup port operations.

c) HHS will issue taskings that draw upon funding from the responding HHS plan agencies.

4. Environmental Protection Agency

As directed in PDD-39, the Environmental Protection Agency (EPA) will activate techni cal operations capabilities to support the Federal response to acts of WMD terrorism. EPA may coordinate with individual agencies identified in the National Oil and Hazardous Substances Pollution Contingency Plan (NCP) to use the structure, relationships, and capabilities of the National Response System as described in the NCP to support response operations. If the NCP is implemented:

a) The Hazardous Materials On-Scene Coordinator under the NCP will coordi nate, through the ESF #10 Hazardous Materials Chair, the NCP response with the FEMA official (either the ROC Director or the FCO), who is responsible under PDD-39 for on-scene coordination of all Federal support to State and local gov ernments.

b) The NCP response may include threat assessment, consultation, agent identifi cation, hazard detection and reduction, environmental monitoring, decontamina tion, and long-term site restoration (environmental cleanup) operations.

VI. Funding Guidelines

A. As stated in PDD-39, Federal agencies directed to participate in the resolution of ter rorist incidents or conduct of counterterrorist operations bear the costs of their own par ticipation, unless otherwise directed by the President. This responsibility is subject to spe cific statutory authorization to provide support without reimbursement. In the absence of such specific authority, the Economy Act applies, and reimbursement cannot be waived.

B. FEMA can use limited pre-deployment authorities in advance of a Stafford Act decla ration to "lessen or avert the threat of a catastrophe" only if the President expresses inten tion to go forward with a declaration. This authority is further interpreted by congressional intent, to the effect that the President must determine that assistance under existing Federal programs is inadequate to meet the crisis, before FEMA may directly intervene under the Stafford Act. The Stafford Act authorizes the President to issue "emergency" and "major disaster" declarations.

1. Emergency declarations may be issued in response to a Governor s request, or in response to those rare emergencies, including some acts of terrorism, for which the Federal Government is assigned in the laws of the United States the exclusive or preeminent responsibility and authority to respond.

2. Major disaster declarations may be issued in response to a Governor s request for any natural catastrophe or, regardless of cause, any fire, flood, or explosion that has caused damage of sufficient severity and magnitude, as determined by the President, to warrant major disaster assistance under the Act.

3. If a Stafford Act declaration is provided, funding for consequence management may continue to be allocated from responding agency operating budgets, the Disaster Relief Fund, and supplemental appropriations.

C. If the President directs FEMA to use Stafford Act authorities, FEMA will issue mis sion assignments through the FRP to support consequence management.

1. Mission assignments are reimbursable work orders, issued by FEMA to Federal agencies, directing completion of specific tasks. Although the Stafford Act states that "Federal agencies may [emphasis added] be reimbursed for expenditures under the Act" from the Disaster Relief Fund, it is FEMA policy to reimburse Federal agencies for eligible work performed under mission assignments.

2. Mission assignments issued to support consequence management will follow FEMA s Standard Operating Procedures for the Management of Mission Assignments or applicable superseding documentation.

D. FEMA provides the following funding guidance to the FRP agencies:

1. Commitments by individual agencies to take precautionary measures in antici pation of special events will not be reimbursed under the Stafford Act, unless mis sion-assigned by FEMA to support consequence management.

2. Stafford Act authorities do not pertain to law enforcement functions. Law enforcement or crisis management actions will not be mission-assigned for reim bursement under the Stafford Act.

VII. References

A. Presidential Decision Directive 39, U.S. Policy on Counterterrorism (classified). An unclassified extract may be obtained from FEMA.

B. PDD-39 Domestic Deployment Guidelines (classified).

C. PDD-62, Protection Against Unconventional Threats to the Homeland and Americans Overseas (classified).

D. FBI WMD Incident Contingency Plan.

E. HHS Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological Terrorism.

VIII. Terms and Definitions

A. Biological Agents

The FBI WMD Incident Contingency Plan defines biological agents as microorganisms or toxins from living organisms that have infectious or noninfectious properties that produce lethal or serious effects in plants and animals.

B. Chemical Agents

The FBI WMD Incident Contingency Plan defines chemical agents as solids, liquids, or gases that have chemical properties that produce lethal or serious effects in plants and ani mals.

C. Consequence Management

FEMA defines consequence management as measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, busi nesses, and individuals affected by the consequences of terrorism.

D. Credible Threat

The FBI conducts an interagency threat assessment that indicates that the threat is credi ble and confirms the involvement of a WMD in the developing terrorist incident.

E. Crisis Management

The FBI defines crisis management as measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

F. Domestic Emergency Support Team (DEST)

PDD-39 defines the DEST as a rapidly deployable interagency support team established to ensure that the full range of necessary expertise and capabilities are available to the on-scene coordinator. The FBI is responsible for the DEST in domestic incidents.

G. Lead Agency

The FBI defines lead agency, as used in PDD-39, as the Federal department or agency assigned lead responsibility to manage and coordinate a specific function either crisis management or consequence management. Lead agencies are designated on the basis of their having the most authorities, resources, capabilities, or expertise relative to accom plishment of the specific function. Lead agencies support the overall Lead Federal Agency during all phases of the terrorism response.

H. Nuclear Weapons

The Effects of Nuclear Weapons (DOE, 1977) defines nuclear weapons as weapons that release nuclear energy in an explosive manner as the result of nuclear chain reactions involving fission and/or fusion of atomic nuclei.

I. Senior FEMA Official

The official appointed by the Director of FEMA or his representative to represent FEMA on the Command Group at the Joint Operations Center. The Senior FEMA Official is not the Federal Coordinating Officer.

J. Technical Operations

As used in this annex, technical operations include actions to identify, assess, dismantle, transfer, dispose of, or decontaminate personnel and property exposed to explosive ord nance or WMD.

K. Terrorist Incident

The FBI defines a terrorist incident as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

L. Weapon of Mass Destruction (WMD)

Title 18, U.S.C. 2332a, defines a weapon of mass destruction as (1) any destructive device as defined in section 921 of this title, [which reads] any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one-quarter ounce, mine or device similar to the above; (2) poison gas; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Emerging Technologies for Response to Weapons of Mass Destruction

Joseph Rosen, MD

The major focus of this report is to identify emerging technologies that can be used to respond to terrorist threats. We are particularly interested in emerging technology that can be used for education, training, simulation, and predicting the outcomes of our operational plans. From our initial meeting in July our goal was to produce a number of recommendations. We further refined these recommendations in a September meeting. Following that, in a series of meetings in October and November, we further refined these recommendations through meetings with operators, policy makers, and technologists.

We took a paper by David Franz and expanded it with input from a small ad hoc group in our September meeting. Included in our list of recommendation are: (1) Technology base: research and development; (2) Intelligence and surveillance; (3) Forensics; (4) Proactive deterrence; (5) Medical countermeasures; (6) Physical countermeasures; (7) Public Health infrastructure; (8) Interagency collaboration; (9) Education; (10) Complementary programs; (11) International cooperation; and (12) New technologies. Our white paper in this section goes into each of these areas in more depth. White papers in our edited volume and references that we cite also go into each of these areas in more depth.

However, our overarching recommendation is to use virtual reality and advanced simulators to create a comprehensive system for counterterrorism. This would be enabled through the creation of a large-scale virtual reality simulation environment as a national center that would integrate our policies, operational plans, emerging threats, and responses within a single framework. The center would exist in cyberspace and have multiple sites throughout the country that could interact on a frequent and on-going basis.

It would take advantage of emerging technology over the past decade that has allowed both the civilian and defense communities to simulate and train for difficult and unusual tasks. The simulation center concept is built upon emerging technologies that have been developed over the past ten years in both the civilian and defense communities (see NAS report on virtual reality 1995, and Nasal Studies Board report 1997 that covered the timeline between 2000 and 2035 and the DMSO web site).

Information technologies combined with virtual reality can be used to create an environment that will allow us to test out our concepts in counterterrorism. In particular, it will allow us to connect our policy and strategy to our operational plans, providing rapid proof by concept analyses of emerging technologies, and demonstrating the role they can play in our antiterrorist efforts. Emerging technologies for responses can be introduced into our simulated worlds to test if they can affect significant improvements in our operation plans.

Simulators have been designed and implemented for small engagements and large-scale event training. Simulators that have been developed to train small engagements of individuals in difficult tasks have been used for flight simulation, urban warfare, and medical response teams. The medical training of first responders in a bioweapons attack could be crucial to the success of providing vaccines and antibiotic treatments when indicated.

Large-scale simulators have been used to model entire battles involving large numbers on manned vehicles for the Gulf War (73 easting/DMSO), by the army, air force, marines, and navy. Their time scales can be real time, or can be altered to allow high levels interactions. A large-scale simulator has not yet been used for simulating mass casualty events for the Department of Justice.

In these simulators, virtual humans are used to simulate casualties, terrorists, and first responders. Their simulators can act according to some predetermined script, or they can be operated or controlled by people assigned to manipulate them for the training session. Some of the virtual humans have been developed to accurately simulate the effect of conventional weapons injuries. For example, they could predict the effect of a gun-shot wound to the leg — the ability of the wounded individual to survive and walk, and how best to repair or stabilize the injury.

Simulators can be used in the actual performance of the task. A simple example of this is in remote operations or tele-operations. In tele-operations, simulators can first be used to practice a task. They then can be used in the performance of the task. In the first case the environment is completely modeled. In the tele-operated case the model can be super-imposed on the actual physical reality. This is often referred to as augmented reality or datafusion. It is used in neurosurgery and is also used in special military exercises. It allows soldiers or surgeons to seamlessly transfer their training from a practice case to the real case.

When operators, such as first responders, are being assisted by virtual mentors that appear within their environment, it is called tele-presence. The experts are located at a distant remote safe site and can supervise and advise the actions of first responders who have less knowledge. This is used now in both civilian medical applications and in military applications. When the expert controls a robot, it is called tele-robotics and requires significant bandwidth between the remote site and the site where the robot is providing assistance. At the present time, remotely controlled robots are being used by the justice department for the de-fusing of bombs and in special cases of hostage rescue.

These technologies were first developed for applications to the management of hazardous materials using tele-operations. They have more recently been greatly advanced for telesurgery. These new systems have realistic 3D vision, 3D sound, and sensitive force feedback touch and manipulation interfaces. They are being used more and more in surgery in remote operations. These systems can be used for training, performance of surgery and, in special cases, have been adapted to allow the prediction of outcomes. These performance machines can allow the surgeon to predict what the effect of a specific maneuver would have on the outcome of the patient. The earliest of these systems was developed in the 1990s. It is based on a physical model of the organ or structure being operated on and measures the effect of a set of events on the outcome to the human body. They can also be used to predict the effect of ballistic weapons on the human body.

We recommend the use of virtual reality simulators to bring together the three parts of the counterterrorism system the policy makers, the operators, and the technologists. We then propose that multiple scenarios be tested within these simulation environments to determine the strengths and weaknesses of our operational plans. For example, the template system for a response to a bioweapons attack that is proposed by Dr. Hutchinson could be tested extensively in this system to determine how it could be employed and adapted to different cities. We can see what the effects of specific emerging technologies would be on our response to specific emerging threats. For bioweapons and mass medical casualties we present this simulation system in the white paper entitled MEDNET. With respect to an augmented reality system we present this system in the white paper CYBERCARE. We also included a paper describing an extreme information infrastructure (Bobby Hartway), and a a paper describing cybercare robots (Neil Fisher). These are all possible physical and information technologies that could be used to respond to a large scale strategic terrorist attack and could be tested within an advanced simulation environment.

POSSIBLE TERRORIST USE OF MODERN BIOTECHNOLOGY TECHNIQUES

Raymond A. Zilinskas, Ph.D.

Introduction

In early 1999, the Center for Counterproliferation Research at the National Defense University (NDU) began a collaboration with the Center for Nonproliferation Studies, Monterey Institute of International Studies (MIIS) to assess the likely impact of recent and anticipated advances in biotechnology on the ability of terrorists to acquire and employ biological agents.

The forecasting method selected for this project was to use a focus group. A focus group consists of experts brought together to consider a series of issues needed to address the subject of concern. The focus group approach is useful for identifying areas of consensus or disagreement on presented issues. The NDU/MIIS focus group, which included both natural and social scientists, possesses a wide range of expertise. However, most of its members are researchers working in the biological sciences; they are affiliated with academic institutions, industry, and government agencies (see Annex 1).

The focus group was asked to consider the possibilities offered by the advanced techniques of biotechnology to terrorist or criminal groups (hereafter combined under the single heading of "terrorists") in the next five years, i.e., up to 2005, to the weaponization of pathogens and toxins. Specifically, the focus group was tasked to:

- analyze newly developed and emerging biotechnology techniques in terms of their utility in research and development (R&D) aiming to produce microorganisms of terrorist utility.
- determine the level of training required by persons who would employ these techniques and the equipment and facilities they would require to do their work.
- concentrate on possible applications directed against human populations.

A draft report containing the findings of the focus group has been written; it currently is being reviewed by outside experts. We expect to incorporate the suggestions by these experts and issue a final report in early 2001. Due to the sensitive nature of some of its descriptions and findings, it will be distributed only to government agencies. A less sensitive version of the report will be published later.

For the purposes of this meeting at Dartmouth, I abstract focus group findings in three areas: (1) attributes of microorganisms that a bioweaponeer would find profitable to enhance; (2) advanced biotechnologies that may be used for that purpose, and (3) main conclusions and recommendations made by the focus group. I end with a short paragraph that discusses two issues that flow from our work and that the Dartmouth conference might consider.

I. Weaponization of Microorganisms

The five attributes that characterize a "perfect" military biological warfare (BW) agent have already been identified. They are as follows:

- High virulence coupled with high host specificity;
- High degree of controllability;
- High degree of resistance to adverse environmental forces;
- Lack of timely countermeasures to the attacked population;
- Ability to camouflage the BW agent with relative ease.

Some of these attributes might not be so important for BW agents that will be applied for terrorist purposes. For example, an apocalyptic terrorist group might be unconcerned whether or not the agents it uses can be controlled after release. Nevertheless, these criteria served as a useful starting point for our considerations of the scientific objectives scientists working for bioterrorists may have when applying modern bioscience and biotechnology to weaponize microorganisms. Thus, to develop "perfect" BW agents, modern biotechnology techniques may be applied to enhance any or all of eight characteristics or traits of microorganisms — hardiness, resistance, infectiousness, pathogenicity, specificity, detection avoidance, senescence, and the viable but non-culturable state.

A. Hardiness

Hardiness refers to the ability of a microorganism or a bacterial or fungal spore to tolerate being enclosed in a storage container or munition, withstand forces used for its dispersal, and, after release onto the target, survive physical and chemical stresses encountered in the open environment. A scientist might attempt to enhance the hardiness of bacteria, fungi, and viruses in two ways. First, the scientist could try to enhance the organism's ability to resist desiccation, withstand ultraviolet (UV) radiation from the sun, and endure decontamination procedures. If successful, the BW agent would survive longer after release, thereby increasing its potential for causing casualties. Second, an attempt may be made to stabilize genetically determined traits, such as virulence, in the weaponized agent. If this was done, the agents constituting payloads of biological weapons would have a longer shelf life, thus lessening the need to continually reload them with freshly produced agents.

With the germinating cells of bacteria, hardiness depends mostly on the bacterium's repair mechanism; i.e., the quickness and thoroughness with which the bacterium's genetic makeup is able to repair damage caused by stressors to its cell wall, chromosome, and other structures. However, due to inadequate scientific knowledge about the genetic control over repair mechanisms in bacteria and limits to the ability of scientists to transfer multigene constructs from one organism to another, the focus group believes that no scientist will be able to genetically increase the hardiness of a bacterial species before 2005.

In relation to bacterial spores, such as those of Bacillus anthracis, nature has made them hardy for the specific purpose of tolerating environmental stresses. In the next five years, science probably can do nothing to improve on nature with regard to enhancing the hardiness of bacterial spores.

Even less is known about the repair mechanisms of fungi than of bacteria, therefore, no one is likely to be in a position to apply molecular biology techniques for the purpose of increasing the hardiness of these organisms before 2005.

Some viruses, such as the smallpox virus, are exceedingly hardy, being able to withstand desiccation for many hours. But most viruses die within minutes after release into the open environment due to desiccation. It appears that the hardiness of viruses depends mostly on the chemical structure of their outer coat. While it is possible to attempt to alter the outer coat of some viruses to change their presentation (see below), there is insufficient knowledge on how to do so to achieve greater hardiness. Most likely, if an attempt to do so were made, other traits of the modified virus would be degraded, such as invasiveness and virulence. For these reasons, there is little or no possibility of scientists, even when applying sophisticated biotechnology techniques, being able to enhance the hardiness of viruses in the next five years.

B. <u>Resistance</u>

Resistance refers to the ability of a microorganism to defeat the actions of therapeutic drugs, such as antibiotics, and preventives, such as vaccines.

The means by which different microorganisms are able to resist drugs and preventives vary considerably from type to type. In regard to bacteria, a scientist might attempt to develop strains that are resistant to antibiotics used by the target population; if virus, the aim could be to develop viral strains that are unaffected by the enemy's antiviral therapeutic drugs; or if a fungus, an effort could be made to develop a strain that resists fungicides and antifungals. The advantage to the bioterrorist of using highly resistant strains in an attack would be greater casualty generation and higher lethality among those attacked.

Imbuing a bacterial strain with antibiotic resistance is no longer a substantial scientific challenge. Many plasmids with resistance markers are available in ordinary bacterial strains; these may be moved into new hosts using either classical or molecular biology techniques. Having stated this, it must also be made clear that although the development of antibiotic resistant bacterial strains is technically not so difficult, this does not guarantee that the altered strains will be better suited for weapons use than their less antibiotic-resistant relatives. The reason is that the newly developed antibiotic resistant strains may evidence pleiotropic effects (unwanted and unplanned characteristics); i.e., the newly engineered strains will possess not only the desired characteristic of antibiotic resistance, it also will manifest additional but unwanted characteristics that will make it unsuitable for weapons purposes, such as less virulence or hardiness (or both). Pleiotropy is discussed in more detail below.

C. <u>Infectiousness</u>

Infection is the process whereby microorganisms invade and establish themselves within the body of a host. Whether or not a microorganism is able to infect a host depends on the outcome of a series of complex interactions between the invader and the host. The bioterrorist scientist can attempt to enhance the invasive abilities of microorganisms being developed for BW. In general, pathogens possess hydrolytic enzymes that destroy lipids and proteins. Since precisely these chemicals constitute the membranes and walls of the host's cells, they become the targets for a pathogen's attack. Scientists thus may imbue a pathogen with the ability to secrete enzymes that act to circumvent antibodies secreted by skin cells such as Immunoglobulin A (IgA). Another approach would be for a scientist to attempt to enhance the ability of bacterial cells to adhere to the walls of the respiratory or intestinal tracts. In immunocompetent hosts, these tracts are protected by being continuously flushed by fluids and by cells lining the tracts secreting protective substances such as mucus and antibodies. To overcome these defenses, pathogenic bacteria produce special proteins, adhesins or receptors, which bind specifically to receptors (proteins on both interacting cells may be called "receptors") located on host cells. Adhesins and ligands are located either on the bacterial cell wall or on structures that protrude from the cell wall such as pili. Since a substantial amount of information is available in the scientific literature about these substances and how they are produced by pathogens, it is possible that scientists could use this information to design projects aiming to imbue pathogens that normally do not produce adhesins with the capability to do so, and enable pathogens to secrete viscous substances, such as alginate capsule and polysaccharide slime, thereby increasing their ability to adhere to host cells.

All mammals are able to produce a large array of defensive peptides that act to destroy invading pathogens. Two types of peptides, defensins and cathelicidins in particular, are vital to a mammal's defense. Alpha defensins are found in the blood and intestinal epithelia, while beta defensins defend the kidneys, urogenital tract, and skin. If a weapons scientist were able to design a pathogen that possesses proteinases with the ability to destroy these peptides, it could well become a powerful BW agent.

There also might be possibilities for increasing the infection capabilities of viruses. Before being able to initiate infection, viruses must attach to an appropriate receptor on the prospective host's body cells. For example, the human immunodeficiency virus (HIV) produces a special protein (gp120) that attaches to receptors on the T lymphocytes (a type of cell that is part of the body's immunodefense system), thus allowing the virus to enter these cells whose normal function is to destroy invading microorganisms. Similarly, the influenza virus uses a protein called hemagglutinin as a type of adhesin to attach to a receptor on respiratory tract cells. Using information that has been published about viral pathogens, scientists can attempt research that aims to alter the genetic makeup of a virus so it can attach more efficiently to receptors or to receptors that it normally could not, of host cells.

Practically speaking, however, there is little information about how microorganisms penetrate skin. Therefore, no one would be in a position to enhance this particular attribute in a pathogen or to transfer the gene (or genes) that controls it from one organism to another. More is known about adhesins and their genetic control. However, it is not known whether the gene-controlling adhesion in one microorganism would be expressed in another microorganism. Further, even if such a gene was expressed, it is possible that the gene transfer would result in pleiotropic effects. Therefore, laboratories working for terrorists probably would find research in this area not worthwhile.

D. Pathogenicity

Pathogenicity refers to the ability of the pathogen, once established within the host, to traverse the bloodstream or lymphatics, evade the intrinsic defenses of the host, enter target tissues of the host, and exert such damage that either injures or kills the host. In general, a pathogen that acts quickly to cause severe damage is considered to be virulent. For example, the smallpox virus and the bacillus causing anthrax are classified as virulent pathogens.

The successful invader's ability to damage the host depends mainly on the operation of a number of virulence factors working in unison to cause damage to the host. It would appear, therefore, that if a scientist were able to add virulence factors to a microorganism being developed for BW, or could enhance a pathogen's intrinsic virulence factors so that they would work more efficiently, the modified microorganism or pathogen would make a better BW agent.

Virulence factors may be grouped under one of three more general headings — local effects, distant effects, and evasion of host defenses.

- Local effects. After taking up residence in a host's tissue, some pathogens secrete enzymes and other substances, such as coagulases, kinases, lecithinases, and proteases, which break down the host's cells and intracellular matrices located proximal to the infectious foci. For example, the so-called "flesh-eating" bacteria are strains of Group A Streptococcus possessing virulence factors facilitating rapidly progressing subcutaneous infection.

- Distant effects. Some virulence factors are released by the established pathogens and are carried by the host's circulatory or lymphatic system to distantly located organs. Among these types of virulence factors, toxins may be of highest importance. Many bacterial pathogens are able to secrete toxins; once these have been liberated and circulate through out the body of the host, they produce fever, shock, and death.

- Evasion of host defenses. Pathogens have evolved numerous strategies to evade host defenses and to utilize substances produced by the host for their own purposes. Thus, many pathogenic bacteria are able to secrete special proteins, called siderophores, which can remove iron from the host's carrier proteins and make it available to the bacterial cell. Some pathogens, such as Streptococcus pneumoniae and Cryptococcus neoformans, produce a glycocalyx capsule that protects the vegetative cell from phagocytosis. There also are species of Staphylococcus and Streptococcus that secrete leukocidins capable of destroying the host's leukocytes and hemolysin and lyzing red blood cells. Some bacteria (such as rickettsias) and viruses (such as HIV and herpes virus) hide within the host's cells, thus evading the host's immune response.

Most virulence factors are proteins secreted by the invading pathogen that act by destroying normal host functions, of which the pathogen then takes advantage. It would appear that the genes controlling the production of some of these proteins would not be difficult to identify and transfer to microorganisms being developed for BW purposes. Quite probably, scientists attempting to weaponize bacteria and fungi would have a plethora of choices as to which virulence factors to use. Further, although viruses are unable to directly secrete proteins, some can be imbued with genes that code for protein production and are expressed when the virus takes over the host cell. For example, scientists were recently able to insert genes, and appropriate promoters, that code for scorpion neurotoxins into a virus used for insect control to improve their insecticidal effectiveness. It would appear that a similar approach could be used to develop more pathogenic viruses for purposes of BW.

It would be fairly easy for an appropriately trained scientist to identify genes coding for many of the well-characterized virulence factors and to transfer these genes from the cells of one bacterial species to another. This is particularly so when a single gene codes for a single protein of importance, such as an adhesin or a toxin. Further, it is well recognized that in some bacterial species, such as Escherichia species and Vibrio species, very small differences in the organism's genome, for example, the absence or presence of a single gene, will determine whether the strain is pathogenic or nonpathogenic. Single genes such as these are easily transferable from one cell to another. It therefore can be concluded that it would be feasible for a bioterrorist scientist to employ the advanced techniques of biotechnology in an effort to enhance the pathogenic potential of well-studied bacterial species through the transfer of genes coding for virulence factors.

In consideration of fungi, much less is known about the pathogenic mechanisms and modes of action than with bacteria. It is therefore highly unlikely that someone will be able to enhance the pathogenicity of fungi within the next five years.

Viral virulence factors are even more mysterious than bacterial and fungal virulence factors. For this reason, it is not probable that anyone will be in a position to deliberately affect viral virulence factors before 2005.

Similar qualifications to those stated at the end of Section B above must also be noted here. While it is not a technically difficult for an appropriately trained scientist to transfer a gene coding for a virulence factor from one bacterium to another, the newly transformed bacterium might exhibit pleiotropic effects that will render it less suitable for weapons purposes than the original strain.

E. <u>Specificity</u>

Specificity refers to a pathogen's propensity to prefer a specific host. A scientist working for bioterrorists might find it useful to either to increase a pathogen's preference for a specified target population or to decrease the pathogen's ability to attack populations other than the target population. By doing so, the probability of a biological weapon causing collateral damage is decreased, thus increasing the bioterrorist's ability to control the weapon.

Host preferences among pathogens vary widely. At the one end of the scale, some species of viruses (for example, certain animal influenza viruses) and bacteria (for example, Mycobacterium lepri) tend to be species specific. At the other end of the scale, there are many bacterial and fungal strains that attack more than one animal or plant species. For example, some subspecies of the bacterial species Pseudomonas aeruginosa can cause disease in every known kind of animal, be it vertebrate or invertebrate, warm-blooded or cold-blooded. Although viruses tend to have a narrow host range, some RNA viruses are capable of using pathways outside their usual host range. For example, the foot-and-mouth virus, which is commonly thought of as only being able to attack cloven-footed animals, recently has been shown to be able to infect and propagate in human cells.

The issue of specificity has become a subject of intense interest during the last few years. There are two reasons for this. First, the Human Genome Project (HGP) will have mapped the entire human genome by 2003 and this information will, to all appearances, be easily accessible to anyone possessing a computer equipped with a modem. One of the implications of this development is that scientists might be able to utilize information generated by the HGP to identify genetic markers specific to certain populations and to perform research for the purpose of developing pathogens or antigens that will preferentially harm individuals possessing these markers.

Second, a host of smaller projects are being undertaken in parallel to the HGP, the goals of which are to map the genomes of viruses, bacteria, fungi, insects, and worms. By late 2000, the complete genomes of about 13 pathogens had been fully sequenced, and another 60 pathogen genomes were well on the way to being characterized. It is reasonable to assume that over a hundred pathogen genomes will have been published by 2005. From the information generated so far by whole-genome research, it is already possible to identify certain genetic characteristics of microorganisms that characterize them as pathogens. The possibility, then, is that scientists may use this information to undertake research with the aim of transforming non-pathogens to frank pathogens or, even creating truly new pathogens.

The biological relationships between hosts and pathogens, be they bacteria, fungi, or viruses, are exceedingly complex, having evolved over thousands or more years. While research on the genetic basis governing some host-pathogen relationships is beginning to produce findings, knowledge about these relationships is still rudimentary. It therefore is the sense of the focus group that it is most unlikely that even the most qualified scientist would be able to enhance the specificity of any type of pathogenic microorganism before 2005.

F. Detection Avoidance

There are two types of detection avoidance. First, it could be the deliberate altering of properties possessed by well-characterized BW agents, such as engineering them to express surface antigens they normally would not express. If so, the target population, using existing methods, would have problems detecting and identifying the modified form of pathogen. Second, an organism could be deliberately altered to defeat the immunological defense systems of a target population.

In reference to the first type of detection avoidance, all known biological threat agents have been characterized to the point that were one of them to be used in an attack, it would be identified within a short time, and appropriate treatment would be administered to exposed populations. Thus, if bacteria are used in an attack, antibiotics would be administered to exposed persons; if viruses were used, it might be possible to administer anti-viral medicines and, if the virus were contagious, institute quarantine and initiate a vaccination campaign to stop further spread. To defeat these defensive measures, a bioterrorist scientist might endeavor to alter a specified organism's antigen presentation, thereby making it difficult for defenders to identify the BW agent through the use of existing detection methods. By doing so, it is likely that the victims of a biological attack would receive delayed, sub-optimal, or erroneous treatment, or a vaccination campaign might not be undertaken in a timely manner.

To develop a bacterial strain that defeats detection by clinical methods, a scientist could attempt to manipulate one or a few genes that control bacterial metabolism or the production of proteins constituting the bacterium's cell wall. By altering a bacterium's metabolic properties, the work of the clinical laboratory to identify the bacterium is made more difficult. If the bacterial cell wall were altered, the modified organism's antigenic presentation would be sufficiently changed to confuse detection methods usually employed in the clinical laboratory to identify organisms to the level of species, such as the polymerase chain reaction (PCR) and mass spectrometry. Similarly, the modified organism might avoid detection by field investigators employing array kits designed to quickly identify any of a number of biological threat agents.

The second type of detection avoidance refers to circumventing primed immunodefense systems of the target population. Human populations of industrialized nations are routinely vaccinated against many common diseases. Shortly after being vaccinated, the vaccinated individuals develop antibodies that most often are able to defeat the pathogens against which vaccines have been developed and administered. In other words, the immunological defenses of vaccinated populations are primed to meet the threat of certain infectious diseases. To defeat this type of defense, a scientist working for terrorists could attempt to genetically engineering a classical threat agent so that its genetically modified form is antigenically different from the parent. If he were successful, the antibodies constituting part of the target population's immunodefenses would not recognize the new antigenic presentation, leaving the host vulnerable to infection by the modified form. In bacteria altering the cell wall, as described above, could do this. With viral species, the scientist could attempt to change the viral coat. Many viruses, especially RNA viruses such as influenza viruses, mutate frequently in nature, in the process changing their antigenic presentation. Research has been, and is being, conducted for the purpose of clarifying how viruses accomplish this; some findings of this research have been published. A scientist might be able to utilize published information in research that aimed to change the antigenic presentation of viruses being developed for weapons use.

Of the two types of detection avoidance, the first type-altering a BW agent's presentation could be done relatively easily by an appropriately trained scientist. However, if genetic manipulations were done on an organism for this purpose, to, for example, alter a cell wall or viral coat, it is almost certain that the manipulated organisms would exhibit pleiotropic effects, such as ending up with a weakened external structure. As has been explained above, the research needed to develop a useful BW agent with altered presentation therefore would be risky, and probably best done by a national program. It also appears dubious that this kind of research would bring significant added value to a BW agent; therefore it hardly would be worthwhile for a terrorist organization to support it.

The focus group believes that research to accomplish the second type of avoidance detection, that of circumventing primed immunodefenses of a target population, is not likely to be done before 2005. The main reason for this conclusion is that before such research could be undertaken, difficult field research would have to be conducted by the future attacker to investigate the immunological status of a target population to be attacked. This would take a long time to complete and probably would not produce findings of sufficient completeness to design an offensive project to develop a BW agent uniquely suited to take advantage of weaknesses or defects found in the target population's immunological defenses.

G. Senescence

Theoretically, microorganisms can live forever. Thus, bacteria and fungi keep subdividing ad infinitum as long as the supply of nutrients is sufficient and their wastes do not accumulate to a toxic concentration, while viruses will survive as long as they can find new host cells that can be programmed to assemble new virions.

Under most circumstances, a bioterrorist can be expected to prefer to have limits on the scope and length of a biological attack orchestrated. If a limited attack were possible, the enemy would suffer, but the probability of the attack affecting friendly or neutral populations would be lessened. One way of limiting the time and/or extent of attack might be by deliberate senescence; i.e., to genetically engineer BW agents to die on cue.

During the last five years scientists have developed sophisticated mechanisms for ensuring that certain genetically engineered microorganisms (GEMs) do not survive after having performed a specified task. To this end, scientists have designed genetic constructs that program the death of the cell into which they are placed under specified conditions. Such constructs, called suicide constructs, typically include a gene that codes for production of a toxin lethal to the host cell and a promoter sequence that activates the toxin gene in response to a precise signal, such as a temperature change or the presence or absence of a specific chemical or nutrient. For example, a recently developed suicide construct allows cells of a biodegrading strain of Pseudomonas putida to survive only in the presence of certain aromatic hydrocarbons that it has been engineered to degrade.

An imaginative weapons scientist might be able to develop a genetically engineered contagious bacterium or fungus useful for BW that contains a suicide construct. The suicide construct would be designed to become activated when, for example, the ambient temperature exceeds or falls below a specified range, or when a certain chemical is encountered, or when a certain chemical is not present. More difficult to accomplish, would be for a scientist working for bioterrorists to develop a suicide construct that activates in a bacterium after it has undergone a certain number of cell divisions or in a virus after it has passed through host cells a certain number of times. If this were done, it would be possible to use contagious pathogens for BW purposes in a controlled manner.

It was the sense of the focus group that although more is becoming known about the natural senescence of microorganisms, and substantial work has been done to design clever suicide constructs, there is still much to learn before it would be possible for anyone to develop a BW agent with controlled senescence. This almost certainly could not be done before 2005.

H. The Viable but Non-Culturable State

Many types of marine bacteria, including Vibrio cholerae (the causative organism of cholera) spend much of life in a state called viable but non-culturable (VBNC) state; i.e., the bacteria are viable but are in a dormant state and cannot be cultured employing standard microbiological technology. Although it is not yet clear why bacteria enter the VBNC state, it has been determined that the VBNC phenomenon is under genetic control. Much research is being undertaken with the aim of clarifying the VBNC phenomenon; some important findings have already been published.

The possibility is that a scientist might try to utilize this information to develop pathogens uniquely suited for biological attacks. For example, if a scientist knew how to cause Vibrio cholerae to enter the VBNC state, he could attempt to suspend a large number of the dormant pathogens in the water filling the bilges of a ship. The ship could be dispatched to the port of the enemy, where it secretly would empty its bilges. At some time determined by, for example, a rise in water temperature or the appearance of certain nutrients in the water, the dormant organisms would revert to their active, pathological state. Anyone consuming seafood, such as fish and shellfish, taken from the area contaminated by the active vibrio would risk contracting cholera.

The sense of the focus group is that a clever scientist would be able to manipulate the VBNC state in a few well-characterized food and water borne agents for purposes of crime or terrorism. With today's techniques it would be possible, for example, to induce the VBNC state in Vibrio cholerae by withholding certain metabolites. The bioterrorist then could contaminate food or beverage with the unculturable vibrios. The metabolite required to bring the organisms out of the VBNC state could be added to, for example, salad dressing. When the salad dressing is applied to salad, the vibrios would revert to their normal pathogenic state, sickening all who had consumed the combination of salad and salad dressing.

The focus group also considered why a terrorist would go through these steps to cause illness among people rather than using an active pathogen directly. There is no ready answer, but it might be that a deranged scientist would do so for reasons that are obscure to us or for the satisfaction of overcoming a technical challenge.

II. Advanced Biotechnology and Microorganism Weaponization

The focus group analyzed three sets of advanced biotechnology techniques that appeared to be of most immediate use to those who would attempt to weaponize pathogens: DNA technologies, genetic and protein engineering, and cell and tissue culture.

A. DNA Technologies

Of the DNA technologies, three merit consideration; gene machines, sequence banks for proteins and nucleic acids, and functional genomics.

i. Gene Machines

A gene is a section of DNA that codes for a defined biochemical function, usually the production of a protein. Instead of cloning genes or assembling them from cloned fragments of DNA, scientists can synthesize genes by using a gene machine (or DNA synthesizer). However, because many genes are longer than can be easily synthesized, a gene usually is assembled from several oligonucleotides (DNA molecules of 100 bases or less). A scientist might use a gene machine to assemble genes that code for the production of desired proteins, such as toxins and virulence factors.

ii. Sequence Banks for Proteins and Nucleic Acids

Bioinformatics is the use and organization of information of biological interest. Much of bioinformatics in concerned with organizing databases that contain this information and making that information available to those who need it. An enormous amount of data are available on DNA sequences, protein sequences, the human genome, enzymes, and other subjects from organizations such as the National Center for Biotechnology Information, the DNA Data Bank of Japan, the Genome Database (GDB) of the Human Genome Project (HGP), and the European Molecular Biology Laboratory. Any scientist who has access to a computer equipped with a modem can access these databases and secure information on genes and proteins of BW interest. Further, a large number of computer software programs have been designed to help scientists utilize the enormous amount of information available for purposes such as designing macromolecules, including toxins.

iii. Functional Genomics

When the HGP ends in 2003 (or sooner), the 80,000 to 100,000 genes that constitute the human genome will have been mapped and this information will be entered into the GDB. Already data generated by the HGP has given rise to a new scientific field called genomic information technology, but more commonly known as "functional genomics." Functional genomics attempts to correlate the activity of a gene with specific activities, such as protein production, disease processes, signaling between body cells, and many others. It has been aptly stated that "The fundamental strategy in a functional genomics approach is to expand the scope of biological investigation from studying single genes or proteins to studying all genes or proteins at once in a systematic fashion." Using functional genomics, scientists are beginning to clarify how genes interact with one another. Most likely, there are many interactions between genes, and between genes and the environment, which control the molecular basis of health and disease.

Scientists working for or on the behest of bioterrorists can, like scientists performing licit research, easily access the GDB. They then might apply functional genomics to identify genetic markers possessed by populations of interest to them. There has been the occasional article in the arms control literature about ethnic weapons (see above), but such ideas have seemed farfetched until now when the HGP is close to achieving its objective. The question is, can information generated by the HGP be used to design biological weapons that selectively affect a chosen population? This question has yet to be answered.

B. Genetic and Protein Engineering

Genetic engineering is a general term for the genetic manipulation or genetic modification of animals, plants, and microorganisms. The oldest, most commonly used, and best-known genetic engineering technique is gene cloning (or splicing), which produces recombinant DNA (rDNA). Simply put, rDNA techniques allow scientists to isolate a gene from the many genes that constitute an organism's genome, and amplify it so it can be examined, altered, and/or emplaced in the genome of another organism. The final step, that is of inserting a gene taken from one organism into another, can be performed using any one of a number of methods, including transfection, transduction, transformation, biolistics, electroporation, and microinjection. The host organism is said to have been transformed after it has received the foreign gene. If all goes well, the transferred gene performs the same function in the new host cell as it did in the cell from whence it originated.

Site-directed mutagenesis is a variant of genetic engineering. It has two steps. First, a construct consisting of the modified gene flanked by DNA homologous to a certain region in the intended host cell is created. Second, the construct is transferred into the host cell. If done well, the modified gene will be incorporated into the cell genome by homologous recombination, and cells successfully transformed in this way can be selected from a population of non-transformed cells. Through the use of this technique, scientists are able to modify the structure of a gene whose nucleotide base sequence is known, by changing a specific base or series of bases.

Protein engineering is the modification of the chemical structure of a naturally occurring protein. This procedure might be done for such purposes as making the molecule more stable, altering the pharmacological properties of the parent protein, or, if the protein is an enzyme, changing its substrate specificity. Further, protein engineering can be done in order to produce a new type of protein, one that is not found in nature, but this is a difficult and lengthy process. Protein engineering therefore is done using existing natural proteins as a starting point.

Scientists employed by terrorists conceivably could use both techniques when weaponizing pathogens. For example, it has been alleged that scientists who worked for the former Soviet Union's BW program used rDNA techniques to combine certain genetic characteristics of the vaccinia and Ebola viruses. Site-directed mutagenesis may be employed in order to change the structure of proteins constituting a bacterium's cell wall so that the modified organism is more difficult to identify or will no longer be recognized by an immune system primed to defend against the parent organism. It should be noted that manipulating microorganisms in this way might also change other characteristics, making them less favorable for production or weaponization (see discussion on pleiotropic effects, below).

Protein engineering might be used by a weapon scientist to develop various toxins for weapons purposes. Genes for a sizeable number of toxins have been cloned, the regulation of the expression of these genes are well understood, and the three dimensional structures of most of these toxins have been clarified. This information is being used in the pharmaceutical industry to develop new vaccines and toxoids. However, this same information could also be used by weapons scientists to develop more stabile toxin molecules so they better resist the action of chlorine, do not dissociate if placed in water, resist heat at the temperature of cooking, and other purposes. Further, as many toxins consist of two subunits (one subunit that ferries the toxin molecule to the cell and/or anchors the molecule to the cell membrane, and a second subunit that acts on or affects the host cell), the possibility exists that protein engineering could be applied to alter a toxin's chemical structure for the purpose of increasing the toxic efficiency of one or both subunits.

Our discussion of the genetic engineering of microorganisms must make mention of pleiotropic effects. Pleiotropy has been a common problem with genetically engineered organisms that have in the past been developed for specific civilian purposes, so there is good reason to believe that similar difficulties are going to beset scientists developing genetically engineered bacteria for terrorist purposes.

Since it is possible, or even likely, that any genetic manipulation of a pathogen done for the purpose of increasing its value as a weapon will also imbue the manipulated organism with unwanted characteristics, the modified organism would have to be field tested before its weapons value could be guaranteed. This kind of activity is not easy to do and, further, outsiders might detect it. To test for virulence, for example, the developer of the agent probably would have to use animal models or, covertly, human beings, before the agent's increased value for weapons use could be ascertained. If a pleiotropic effect were noted that decreased the modified organism's value for weapons use, further research and experimentation would have to be done by the developer to remove the unwanted pleiotropic effect while retaining the modified organism s added property. The implication of these uncertainties is that genetic engineering research undertaken for the purpose of enhancing a microorganism's utility for weapons use is risky for two reasons. First, it might fail. Second, even if an organism with apparently enhanced properties were developed, there is a substantial possibility that pleiotropic effects would become manifest in the modified organism, necessitating further research, development, and testing to remove them. It could take a long time and considerable effort before an organism exhibiting superior qualities for weaponization were developed, and in the end the entire effort might fail.

III. Concluding Thoughts

The focus group established by the NDU and MIIS grappled with the question of when we can expect that results from applications generated by advanced biotechnology will become realized for terrorist purposes. It concluded that by 2005, few such applications are likely to appear. Those few pertain to scientists working for bioterrorists would be able to develop bacterial pathogens possessing increased resistance against antibiotics, being imbued with added virulence factors, having altered antigenic presentation and, perhaps, being made more controllable through the VBNC phenomenon. However, due to possible pleiotropic effects, none of these properties will necessary result immediately in the modified organism becoming more suitable for weapons use.

Keeping these uncertainties in mind, it is the sense of the focus group that two types of bioterrorists are in the best position to apply the advanced techniques of biotechnology in research to enhance microorganisms for purposes of BW. The first type consists of states possessing BW programs and supporting international terrorist groups. Given that these state programs can be assumed to be staffed with qualified technicians and scientists, well funded, and designed to operate for the long-term, they are most able to undertake the type of risky R&D described above and to perform adequate field testing that would ascertain the newly developed agent's value for weapons use.

While it is impossible to forecast the exact reasons that a nation would want to equip its dependent terrorist group with weapons whose effects depend on genetically engineered weapons, two possible reasons are: (1) just before the government of the terrorist-supporting nation initiates general hostilities against an enemy nation, it could order its dependent terrorist group to use biological weapons against that nation for the purpose of killing its leaders, demoralizing its military forces, and spreading panic and confusion among its civilian population. If used in this kind of attack, the biological weapon equipped with the enhanced organism could be expected to cause a higher number of casualties then a classical BW agent; and (2) the terrorist-supporting nation may feel that it is not strong enough to fight an enemy nation using conventional arms, but nevertheless wants to harm the enemy nation for reasons of revenge, jealousy, etc. For example, governments of nations such as Cuba and Iraq have indicated strong grievances against the U.S., but are too weak to seek recourse by traditional military means. Knowing how powerful and damaging biological weapons are, they might vent their frustration by ordering their dependent terrorist group to carry out a biological attack. If done correctly, not only would the attack cause terrible damage and harm, but also there would be little risk of the responsible party being identified. In this type of attack, the genetically engineered organism might be designed to cause high casualty rates and to be difficult to detect and identify.

The second type is the disgruntled or deranged scientist who works in a well-equipped clinical microbiology laboratory or academic laboratory involved in some aspect of microbiological research. This kind of person can be expected to have the knowledge, patience, and resources needed to undertake and complete the research perceived as needed to accomplish the objectives and to do the testing necessary to ascertain the newly developed agents value for weapons use. The disgruntled scientist might wish to get back at someone or some organization and would use a new strain of microorganism developed by himself to do so. This organism might be more deadly, or more difficult to treat, or have specific effects. The deranged scientist might undertake to develop a particularly clever and vicious organism just to demonstrate that he can do it. Lest someone believes that this seems farfetched, regard present-day computer hackers. Some of them demonstrate how clever they are by designing and dispersing destructive computer viruses; the proof of their cleverness is the amount of damage their creations cause to people who have never harmed them in any way.

While recognizing that it is a chancy endeavor to predict developments that might occur during 2005 and 2009, certain research currently being done could give rise to findings applicable to a much greater degree than was formerly the case in the development of BW agents. The implications of research for BW particularly needs monitoring in six areas: (1) human functional genomics; (2) bacterial functional genomics; (3) pathogenicity islands; (4) synthetic viruses; (5) synthetic mycoplasmas; and (6) fusion proteins. In view of the rapid advances that we have seen in these areas during the last few years, assessments such as the one done here should be repeated every two years.

IV. Possible Issues for Discussion at the Dartmouth Conference

As far as I know, the problem of pleiotropic effects has never before been discussed in meetings addressing bioscientific advances that may be used for purposes of biological warfare and weaponry. There have been many statements made on how genetic engineering can be used to enhance the pathogenic properties of microorganisms, but not on the problems that might accompany such manipulations. If these problems turn out to be minor, then advanced biotechnologies hold real promise to those who wish to use them for weapons purposes. If the problems are major, it is one less aspect of biological weapons development for us to worry about. Which is it?

Closely related to the foregoing is the matter of "field testing." By far, new products developed for peaceful purposes are extensively tested in the laboratory and the field before they are marketed. Would the scientists and technicians working for terrorists have the time, resources, and patience needed to perform testing before their new creations are unleashed? If not, there is a substantial possibility that their creations will fail when used in attacks. How do we address failed attacks? Indeed, how do we determine whether a failed attack has taken place? As far as I am aware, this issue has never been addressed.

Annex 1: Members of the NDU/MIIS Focus Group

Dr. Ken Alibek
Dr. Seth Carus (co-chair)
Dr. Rita R. Colwell
Dr. Rolf A. Deininger
Dr. David Franz
Dr. Donald A. Henderson
Dr. Raymond Kaempfer
Dr. Scott Lillibridge
Mr. Milton Leitenberg
Dr. Lawrence Loomis
Dr. Charles E. Main
Dr. Allan J. Mohr
Dr. Steven S. Morse
Dr. Drew Richardson
Mr. Masaaki Sugishima
Dr. Jurgen Von Bredow
Dr. Mark L. Wheelis
Dr. Raymond A. Zilinskas (co-chair)

Endnotes and References

1. For purposes of this study, biological agents are taken to include both living organisms and toxins.
2. The focus group did not consider classical microbiology except to provide background and for the sake of comparison between old and new approaches.
3. The focus group did not consider biological weapons that may be used against animals, plants, or inanimate objects.
4. Zilinskas, R.A., 1986. "Recombinant DNA Research and Biological Warfare," in R.A. Zilinskas & B.K. Zimmerman, The Gene Splicing Wars: Reflections on the Recombinant DNA Controversy, (New York: Macmillan Publishers), pp. 167-203.
5. Harrison, R.L. and B.C. Bonning, 2000. "Use of scorpion neurotoxins to improve the insecticidal activity of Rachiplusia ou multicapsid," Biological Control 17(2):191-201.
6. Currently, indications are that intragroup genetic variability is greater than genetic variability between groups. Nevertheless, information generated by the HGP is likely to eventually identify specific genetic differences between populations.
7. Integrated Genomics Inc. GOLD: Genomes OnLine Database HomePage, http://216.190.101.28/GOLD/,September 20 (2000).
8. PCR is a method for rapidly amplifying a small amount of genetic material to such an extent that it can be easily identified.
9. Some investigators now believe that the human genome contains more genes than previously thought, perhaps as many as 140,000.
10. Hieter, Philip and Mark Boguski, 1997. "Functional genomics: it s all how you read it," Science 278:601-602.
11. Some claim that Soviet scientists combined smallpox and Ebola viruses (see Preston, Richard, 1998. "The bioweaponeers," New Yorker, March 9, pp.52-65). This probably did not happen. However, the techniques used for the genetic manipulation of the vaccinia virus would not differ from those that would be used to genetically manipulate the smallpox virus.
12. Del Giudice, G. and R. Rappuoli, 1999. "Genetically derived toxoids for use as vaccines and adjuvants, Vaccine 17:S44-S52.

Application of Gene Therapy Strategies to Offensive and Defensive Biowarfare

Christopher H. Lowrey, M.D.

Principles of Gene Therapy

Genes are stretches of DNA which contain the information necessary for the cells of all living organisms and viruses to make specific proteins. Proteins, in turn, perform most of the necessary functions of the living organism such as digesting food, conducting nerve signals, carrying, helping fight infections, moving muscles, etc. Gene therapy involves the expression of a gene or genes within a patient's specific target cells which change the functional properties of the cell such that a therapeutic benefit is produced for a patient. For example, in a person with sickle cell disease, the adult b-globin gene has a single base pair mutation. This changes the structure and function of the b-globin protein producing a severely debilitating disease in homozygous individuals. The goal of gene therapy for this disease is to replace the defective gene in the patient's blood cells with a normal gene so that the normal hemoglobin protein can be produced. Another, perhaps more relevant example of gene therapy involves strategies to treat cancer. These include putting genes which code for proteins lethal to cells, into cancer cells; placing genes into cells which make them resistant to toxic agents (i.e., chemotherapy) or altering the function of the cells of the immune system so that they more efficiently kill cancer cells.

While relatively simple in concept, the goal of putting genes into patients' cells has been elusive due to a variety of technical problems which must be overcome before gene therapy will be useful for more than a few relatively infrequent situations. These technical challenges include developing the ability to efficiently transfer the DNA which carries the therapeutic gene into target cells of patients and, once the gene is in place, to get it to express (make the protein it codes for) at high enough levels to be of therapeutic benefit. Over the past several years significant progress has been made in overcoming these and other technical hurdles to successful gene therapy. However, the very discoveries which will make gene therapy a viable strategy in the near future may also be applied to the development of novel biological weapons or the upgrading of current weapons so that they are able to circumvent current defensive strategies. Conversely, gene therapy strategies may also be applied to protect targets from specific bioweapons. Specific examples of such strategies are presented below.

Possible Offensive Applications of Gene Therapy Strategies to Biowarfare

A paradigm for biological weapons is the use of pathogenic viruses or bacteria to infect targets. Potential defenses against such agents include antibiotics or vaccines to suppress the development of infections by these agents or the use of immunologic or pharmacologic agents to suppress the effects of toxins that are produced by the pathogens. Some of the ways in which the technology currently being developed for gene therapy could significantly impact on this model of biowarfare are described below.

1.) Use of drug resistance genes.

A strategy used in the gene therapy of cancer is to transfer genes which confer resistance to certain toxic drugs (chemotherapeutic agents) to the normal cells of a patient. For example, if the dose of a certain chemotherapeutic agent used to treat lung cancer (for example) is limited by its toxicity to blood cells, then a gene which protects cells from the chemotherapeutic agent could be put into all blood cells. The blood cells would then be resistant to the chemotherapy drugs so that higher doses could be used to achieve more effective killing of cancer cells. Examples of proteins which protect cells from chemotherapy drugs include enzymes which break down the drug inside cells, protein pumps which are able to export toxic drugs out of cells, and proteins which allow the cells to keep growing despite the damaging effects of the drug. Technology currently available for gene therapy and molecular biology could easily be adapted to transfer protective genes to pathogenic bioweapons such as bacteria and viruses, thus making them, or the cells they infect, resistant to drugs which might combat the warfare agents.

2.) Alteration of toxin genes to potentiate biologic damage.

Another strategy in gene therapy is to replace genes which code for abnormal proteins with genes which code for proteins with normal or even improved functional properties. Genes coding for toxins of pathogenic microbes could be isolated and engineered *ex vivo* to produce proteins with altered properties. One example might include toxins which bind more strongly to a cellular target and thus produce a more potent response. Another might involve a toxin for which a specific pharmacologic inhibitor had been designed. The gene, and therefore the protein structure, of the toxin could be altered so that it was now resistant to the antidote, but was still able to carry out its toxic function. Using gene therapy-derived gene transfer techniques, these genes could then be returned to the parent microorganisms, thus making them more effective biological weapons.

3.) Alteration of genes to help microorganisms elude vaccine strategies.

One current defensive strategy against infectious bioweapons is to vaccinate potential targets so that an immune response is developed to the agents. These strategies result in the production of antibodies which can bind to and inhibit the function of biotoxins or kill the microorganisms which produce them. Similarly, vaccines can also lead to the development of specific immune system cells (lymphocytes) which destroy invading microorganisms. Vaccines to specific organisms or the toxins they produce can potentially be administered to persons to elicit immune responses to these agents. The antibodies and lymphocytes which mediate these responses specifically recognize structural features of the microbe or toxin and destroy it. Using molecular biological techniques, the genes for these immunologic targets can be isolated, modified so that they are no longer recognized by the target's immune system, and returned to the parental microbe to produce an altered strain of the organism which will not be recognized by the immune defenses of a vaccinated target.

4.) Transfer of toxic gene products from one infectious bioweapon to an alternative bioweapon.

A specific antibiotic, vaccine, or other strategy might be developed against an infectious, toxin-producing bioweapon making that weapon ineffective. Using methods adapted from gene therapy, the gene coding for the toxin could be identified, isolated, and inserted into a new microorganism (for example a different bacteria or a virus), thus delivering the same toxin with a different vector.

5.) Transfer of a non-microbial toxin gene into a microbe.

The gene for a non-microbial protein toxin (such as a snake, fish, or spider venom) could be inserted into the genome of an infectious agent (such as a bacteria or a virus) so that the toxin would be produced within the target's cells. Multiple toxin genes could also be inserted into the same vector to increase toxic potential.

6.) Changing the tropism of an infectious bioweapon.

Many infectious agents infect specific cells within the human body by binding to proteins on the surface of the target cells. This binding to specific target cells is mediated by specific proteins on the surfaces of the viruses or bacteria. By exchanging the genes which code for these microbial proteins, the normal target tissues of the weapon could be changed so that a new organ can be targeted. For example, a virus that normally infects the liver and needs to enter a person s blood stream to be effective could be altered to target lung tissue so that it could be administered by inhalation.

7.) Development of novel infectious agents.

In order to create more effective viruses to transfer therapeutic genes, new versions of viruses have been developed from which many or most of the viral genes have been removed and then replaced by the gene or genes to be carried. While in many cases this has been done to remove genes coding for virulent proteins, similar manipulations could be performed to enhance the virulence of a virus. For example, genes coding for multiple toxins could be inserted into viruses. Another example is that a disease-causing virus such as the AIDS virus could be made more virulent by the addition of a toxin or by changing the viral surface proteins so that the virus is resistant to vaccines.

8.) Transfer of genes without microorganisms.

Because of potential hazards and inefficiencies involved with the use of microorganisms as vectors to transfer genes in gene therapy, several strategies have been developed in which DNA-carrying genes can be transferred directly into a patient's cells without the need of a virus or other biologic vector. These techniques include the injection of gold particles coated with DNA into a person's skin, and direct injection or inhalation of naked DNA or DNA complexed to lipids. While these strategies are not likely to be applicable to large scale bioweapons, they might be effective as local weapons. One could envision the transfer of a toxin-producing gene into a target, or the introduction of a gene that might cause cancer or other serious illness in a target several months or years after the initial attack.

9.) Regulated expression of toxic genes.

In certain gene therapy applications it is advantageous to be able to turn genes which have been delivered to a patient, on or off at specified times by the administration of a drug. Such systems have already been developed and are being employed in models of gene therapy. These could be used as part of a controlled or clandestine bioweapons strategy where targets could be infected with a virus (for example) carrying a toxic gene. The gene would lie dormant inside the target's cells until the signal, for example, a common antibiotic such as tetracycline, was administered to the target of the bioweapon. This would then activate the gene and produce a lethal response.

Possible Defensive Applications of Gene Therapy Strategies to Biowarfare

Due to the high degree of plasticity of biologically-based weapons, the use of gene transfer concepts seems more applicable to offensive strategies. They may, however, also be used defensively. Two examples are given below.

1.) Vaccine Development

Vaccines are among the most potentially effective protective mechanisms against microbiologic weapons and toxins. However, concerns over the safety of vaccines based on the actual organisms remain. One way around this would be to use vaccines based on the genes or proteins of the microorganisms. Gene therapy experiments have demonstrated the feasibility of vaccinating people with very small quantities of DNA which code for microorganism proteins. The DNA is taken up by the person's cells, the protein coded for by the gene is made, and the body then develops a potent immune response to the foreign protein, thus offering protection against the intact microorganism even though only a small piece of DNA has been administered to the person. Similarly, small pieces of protein derived from a microorganism can be administered to elicit an immune response. These DNA fragments can be produced efficiently and inexpensively, and administered safely to subjects. As this technology is further developed, the possibility of rapid responses to new biowarfare agents can be envisioned. While such applications are likely to be more than an decade away, identification of a new bioweapon, sequencing of its genome, prediction of potential cell surface antigens from the sequence data, and the subsequent derivation of DNA-based vaccines, could conceivably be accomplished over a relatively short time span (i.e., days) to rapidly produce a protective vaccine.

2.) Production of Protective Gene Products Within Targets Cells.

Most bioweapons work by producing proteins which somehow damage or kill the cells of the target. Bacterial toxins are one example of such proteins. Another would be viral proteins which induce the death of cells they have infected. A common strategy used in molecular biology research is to make artificial genes which direct the production of artificial proteins that inhibit the functions of other proteins. These are termed dominant negative proteins and are usually structurally similar to the normal protein. Dominant negative proteins could be devised to inhibit the functions of critical proteins produced by bioweapons (including the offensive examples given above). Genes coding for these proteins could be delivered to the target's cells using gene therapy technology.

Summary

Gene transfer into patients' cells was recognized as a potential medical therapy more than 30 years ago. Only now, after many years of intense investigation, is gene therapy beginning to produce beneficial results in the clinic. While many strategic applications of this technology can be envisioned, the successful development of these strategies is also likely to require the investment of significant resources and time.

The New Battlefield in our City Streets: The Epidemiology of Biological Terrorism in the US and Some Thoughts on the Way Ahead

David R. Franz, Ph.D., D.V.M.

The last 60-70 years of the twentieth century might be called the modern era of biological warfare (BW). During this period, nation states developed biological weapons to be used on a far-away "European battlefield". Even after ratification of the Biological Weapons Convention of 1972, the most impressive BW program in the history of humankind continued for 20 years, effectively cloaked in secrecy. Yet between 1970 and 1990, little thought was given to the possibility of biological warfare or a biological terrorist attack on US cities. Funding for biological defense in the US was minimal and most of the federal government was oblivious to the threat.

In fiscal year 2000, the US government committed more than $1.5 billion to military biodefense and another $1 billion to domestic preparedness for biological attack. What happened? In 1991, the US decisively engaged the Iraqi force, demonstrating vast conventional technical superiority while the world watched on CNN. Shortly thereafter, with economic implosion in the Former Soviet Union, our concern turned to the fate of tens of thousands of Russian scientists and engineers who had developed an impressive program which may never be surpassed in scale or offensive capability. We feared that lesser nations might turn to now jobless Russian bioweaponeers for help in building their "great equalizer." All this occurred with a backdrop of increasing evidence that the dual-use nature of bioweapons programs might make treaties unverifiable. Here at home, the equally dual-use biotechnological revolution screamed forward while novels imprint the horror of bioterrorism on our minds, and experts proclaimed that there are no technical solutions. What can we do?

There is no silver bullet. Our best deterrent and response to the unknowns of bioterrorism must be a broadly integrated defense founded on a deep and sustained biotechnical base. The solution does not lie in procurement of things: such as safety equipment, clothing, or gadgets for fire services or police. If preparation for chemical terrorism is HAZMAT equipment, treatment in the streets, and a cordoned-off crime scene, preparation for biological terrorism is education, a robust public health system, and broad interagency collaboration. The integrated system must include intelligence and forensics, the means and the will to retaliate, medical and physical countermeasures, and a strong public health infrastructure, all bound by vigorous interagency collaboration and effective educational programs. We face a very complex problem; one of low-probability, but potentially high-impact. Calling for a "Manhattan Project" may actually be under-response. What must we do?

1.) Technological base: We believe that we understand the relative limits of nuclear physics and chemistry, but we do not understand the limits of biology for good (medicine), or evil (biowarfare). The future biological warfare or terrorism threat is relatively unknown; therefore, it will be difficult, especially in the medical arena, to prepare specific countermeasures for all threats. We must be capable of responding quickly and effectively to the unknown, therefore, our technical base must be deep and broad. There is not a military-industrial complex for biological defense as there was for our nuclear weapons and energy programs. We must strengthen our military tech-base for threat evaluation, pathogenesis, and specific medical countermeasures research. We must expand and leverage non-military government public health research, especially in the areas of immunology, diagnostics, and drug development. We must increase our support to academic researc, and partner with industry for advanced development and production of orphan vaccines and antiviral drugs. All of these efforts will provide more spin-off application to public health than we typically expect from defense research. Finally, we must demonstrate that we are in this battle for the long term.

2.) Intelligence: Intelligence for bioterrorism is extremely difficult because of the dual-use nature and minimal signature of the weapons programs. Facilities, equipment, and human resources for the R&D and production of biological agents are not unique. Even weaponization and dissemination especially for the terrorist can be done with equipment from legitimate industry. Precursors are not unique and signatures are non-specific, rapidly diluted, destroyed in the environment, or nonexistent. Maintaining quality expertise in our intelligence analyst corps is proving difficult because of competition from industry for our best young scientists and the mundane aspects of the analyst's job. On the other hand, the "new openness" fostered by information technologies and the spread of free enterprise biotech throughout the world offer new options for information mining. We must not only use these technologies to better understand the threat worldwide, but to better use human resources which are more plentiful in this era of increased mobility.

3.) Forensics capability: While diagnostic capabilities are paramount to responding medically to an attack, attribution following bioterrorist attack will require exquisite forensics capabilities. We must be capable of quickly dissecting an organism at the molecular level. More importantly, people who are familiar with the epidemiology and laboratory characteristics of strains and isolates from around the world, and who work with these agents daily, must do this work. Obtaining the complete genetic fingerprint of an agent used in a biological attack will never be as good in the world court as matching rifling marks on a bullet with the criminal's firearm, but without this information we won't have a clue. Even in preparation, what we learn about the genomes of the biological agents of concern will have application in basic science and public health.

4.) The will to retaliate: The way we respond to the first use of biological agents against our citizens, even if it is not a mass-casualty event, will likely set the general course for our future interplay with the biological terrorist. The Israeli model for defense against airline hijacking granted a less complex problem than we face here has proven effective: vigilant, integrated, uncompromising, and swift. We must take the most extreme measures against known proliferators and users of biology to harm our citizens; their clear understanding of our resolve will serve as a deterrent.

5.) Medical countermeasures: Protecting civilians from bioterrorism is more difficult than protecting a military force. For the force, we can use: 1) active immunization for some agents; 2) passive immunoprophylaxis and chemoprophylaxis for others; 3) battlefield detection systems; 4) physical protection (masks); 5) identification and diagnostic tools and methods; 6) decontamination procedures; 7) passive immunotherapy; and 8) chemotherapy. For an attack on our citizens, our useful countermeasures begin with identification and diagnostics and essentially end with chemotherapy.

Identification of the agent used in an attack is of critical importance. Without this, rational post-exposure prophylaxis will be futile. Diagnostic capabilities must be ready in the field, throughout a network of hospital and government clinical laboratories, and in key national reference laboratories. Classical and molecular methods must be known and validated. Triage may be critical to success in therapy of the right subpopulation. Humans exposed, even to replicating agents, will not have measurable amounts of the agent in their blood or serum for several days at the earliest, nor will they have a measurable immune response. Yet, humans or domestic animals may be the only sentinels at the site of an aerosol attack. Therefore, methods of preclinical diagnosis must be developed.

We must consider stockpiling antibiotics effective against anthrax, pneumonic plague, and tularemia. Today, neither antiviral drugs for smallpox, nor vaccines for the two agents smallpox and anthrax for which they might be needed post-attack, are available in sufficient quantities to allow stockpiling. We must leverage industry and academic research which target selected threat agent active sites for antiviral drugs. We must develop adequate stocks of anthrax and smallpox vaccine. Most experts believe that ventilators are likely to be in short supply after an attack on a city, with certain of the most lethal classical agents. We must also prepare for rapid acquisition of necessary equipment and hospital bed space in an emergency. Finally, we must consider and prepare for the potential psychological impact of a biological attack on our primed society.

6.) Physical countermeasures: Fewer physical countermeasure options exist for the civilian population than for the military force. At present, technological hurdles (cost, logistical requirements, narrow spectrum, and high false-positive rates) prevent the widespread application of sensor technologies for biological terrorism. Without timely warning, protective masks seem to have little utility. However, some experts advocate the development of a simple, inexpensive bio-only mask to be carried in automobile, briefcase, or purse. To date, this concept falls below the threshold set by the balance between perceived risk and benefit to the population. Collective protection by modification of HVAC systems in critical public buildings may have utility. Decontamination of patients, buildings and environmental areas must be considered. It is believed that decontamination following a biological event is less important than following a chemical attack. The true aerosol that is required for effective dissemination of a non-volatile biological agent might leave little residual, except around the area of detonation. The agent deposited is thought to be poorly reaerosolized and subject to inactivation by environmental factors, especially ultra-violet light.

7.) Public health infrastructure: Strengthening our public health infrastructure should be at the forefront as we prepare for bioterrorism. Effective surveillance programs, improving the laboratory capabilities at state and local levels, teaching and practicing public health and epidemiology, enhanced communications, and health threat response systems are all dual-use functions. Not only do they prepare us to better respond to a human-made "outbreak", but to a naturally occurring one as well. The current initiative supported by the Public Health and Social Services Emergency Fund for FY2000 is an important start. As with our biomedical tech-base and intelligence programs for biodefense, we must think "long-term" in supporting our public health infrastructure. It will be cost effective.

8.) Interagency collaboration: Preparing to respond to biological terrorism must involve intelligence, law enforcement and other traditional first responders, clinical and research medical communities, public health, political leadership, and the military. It must involve national, state, regional and local organizations, agencies, and officials. As the perceived threat has mounted and the federal government has responded with funds, bioterrorism defense has become a growth industry. Yet, no single office with the necessary authority has clearly taken the lead, either within the Department of Defense or the federal government. Therefore, interagency collaboration has become even more important. Vertical (local through national) and horizontal (across all disciplines) communication and willingness to collaborate are imperative. Excellent leadership facilitates necessary collaboration.

9.) Educational programs: Education and training must be given the highest priority. The fundamental need in a hospital or medical center facing a spike in the patient load following an attack is application of the standard principles of medicine with which the professional and support staffs are already intimately familiar. But our health-care providers have not seen the diseases caused by many of the threat agents. Education and training must include the general characteristics of biological agents versus chemical agents; clinical presentation, diagnosis, prophylaxis and therapy of the most important diseases; sample handling, decontamination and barrier patient care. Training, planning, and drills must prepare physicians and staff for mass-casualty patient management, respiratory support for unusual numbers of patients, and distribution of medications or support of the local government in vaccination programs. Engineering staffs must be taught to establish improvised containment in patient rooms or suites. Traditional first-responders and public and military leaders must understand rather complex technical and biological issues in order to effectively balance cost and benefit in preparation and response. Application of the knowledge we already have though education may be the least expensive and the most important thing we can do as we prepare.

10.) Complementary programs: In addition to the obvious domestic preparedness initiatives needed, we must be prepared, through the military or law enforcement, to destroy biological weapons whether deployed or in storage. We must have the means to neutralize facilities wherever they are found. We must seek and support international law that would bring proliferators to justice. We must seek to enhance communication between scientists internationally, through cooperative threat reduction programs with states that might threaten us; though there are significant risks inherent in these programs, there are huge potential payoffs as well.

11.) New Technologies: We must exploit to the fullest, the phenomenal advances in both biotechnologies and the cyber- and communication-technologies that have occurred in parallel with the changing biological terrorist threat. Genomics and proteomics are revolutionizing diagnostics, vaccine development, and drug discovery. These have obvious and wide application for biodefense. Telemedicine, robotics, virtual reality and simulation, nanotechnology, and the Internet and wireless communications must be used to replace or augment human capabilities and allow us to respond more quickly when lives are threatened. If we keep the pressure on those who would use these breakthroughs for evil taking away their freedom through effective intelligence programs and law enforcement we will be more likely to stay steps ahead as we use the technologies for good, and provide an additional deterrent to the threat.

Bioterrorism presents a daunting problem to our free society, especially at the unique intersection of politics and biotechnology that occurred during the last decade of the 20^{th} century. We may have been lulled by our prosperity and strategic isolation from major conflict into a sense of invulnerability. However, we are vulnerable today and there is no reason to believe that will change in the near future. We must carefully evaluate the real threat, make difficult cost-benefit decisions, and continue to build a fully integrated defense against the distortion of biology by those who would do us harm.

An Assessment of Biological Weapons Threat to the United States

Milton Leitenberg

This paper evaluates the threat of biological weapons use against the United States in the near term. It does this by surveying, successively,

- the proliferation of biological weapons (BW) in identified state programs;
- the historical record regarding the potential for state-supported terrorism with biological weapons;
- the experience of the use of biological agents by non-state groups, either identified as terrorist organizations, or by any other designation; and
- the requirements and parameters for non-state groups to produce biological agents capable of being used as weapons systems.

1. The Proliferation of Biological Weapons since 1972

The questions that should be addressed are:

- How many nations have sought to acquire BW since 1972?
- Which ones?
- How advanced are or were their BW programs?
- Do we have any idea of why these programs were initiated?
- Is there any likelihood that ongoing programs could be reversed and closed down?

Official US government statements repeated for many years that there had been four nations in possession of offensive biological weapons programs in 1972 at the time of of the signing of Biological and Toxin Weapon Convention (BTWC), and that this number had increased to ten by 1989. Beginning in 1989, testimony to Congress by senior US government officials and the annual Non-Compliance statement by the administration to Congress specifically identified these states by name.

These statements additionally noted that some of the states listed were signatories of the BTWC. Israel and South Africa, however, were never mentioned or listed. Israel is omitted from annual U.S. arms control non-compliance statements because it has neither signed nor ratified any of the non-proliferation treaties, including the Biological and Toxin Weapons Convention. It is also omitted entirely in the US Department of Defenses annual report on proliferation of weapons of mass destruction, Proliferation: Threat and Response. No mention whatsoever is made of Israel; in fact, it is not even listed among countries in the report s Middle East section. In any case, what this means is that since Israel is not a BTWC signatory it is technically not in non-compliance, whatever the status of its BW program may be. However it is clear that South Africa maintained an offensive BW program in the past, and Israel did so as well, and presumably continues to do so.

Table 1. States Having BW Programs at Least Approaching Weaponization

	U.S. Government Arms Control Compliance Reports to Congress (1993,1995)	**Admirals Brooks[1], Studeman,Trost 1988,1990,1991; Sec. Cheney, 1990**	**U.S. and UK Governments (1995)[2]**	**Russian Federation [3] Foreign Intelligence Report, 1993**
Middle East				
Iraq	X			X
Libya	X	X		
Syria	X	X		X
Iran	X	X		
Egypt	X	X		
South/East Asia				
China	X			
North Korea		X		X
Taiwan	?	X		
India [4]		X		?
South Korea				?
Africa				
South Africa			X	
Russia	*Ambiguity regarding continuation of offensive program*			

1.) Statement of Rear Admiral Thomas A. Brooks, USN, Director of Naval Intelligence, before the Seapower, Strategic and Critical Materials Subcommittee of the House Armed Services Committee on Intelligence Issues, March 14, 1990, p.54; Statement of Rear Admiral William O. Studeman, USN, Director of Naval Intelligence, before the Seapower, Strategic and Critical Materials Subcommittee of the House Armed Services Committee on Intelligence Issues, March 1, 1998, p.48; Statement of Admiral C.A.H. Trost, USN, Chief of Naval Operations, before the Senate Armed Services Committee on the Posture and Fiscal year 1991 Budget of the United States Navy, February 28, 1990; Remarks Prepared for Delivery by the Honorable Dick Cheney, Secretary of Defense, American Israel Public Affairs Committee, Washington, D.C., June 11, 1990 News Release, No. 294-90, p.4.

2.) The South African government claims that its program was disbanded in 1992. Official British government statements refer only to around 10 nations with or seeking BW, but do not name any countries aside from the separate identification of South Africa in 1995.
3.) Proliferation Issues: A New Challenge After the Cold War, Proliferation of Weapons of Mass Destruction, Russian Federation Foreign Intelligence Report, trans. Joint Publications Research Service JPRS_TND 93-007, March 5, 1993.

In November 1997, the Director of the US Arms Control and Disarmament Agency (ACDA) increased the US estimate to 12 nations (in the course of a statement to negotiating states to the BTWC in Geneva), although the additional two states have never been identified by US officials.

The number is therefore twelve, and not sixteen, seventeen, or eighteen, as are sometimes found in the press. These are offensive biological weapons programs, which the BTWC prohibits, but it does not in all cases mean regular production of biological weapon agents, the storage of stockpiles, or the possession of weapons. Official US or British government statements have further been confounded by the inclusion of caveats such as "suspected", "developing", or "capable of". We have only one example in the public record of what the scale of these differences may be; that statement is ten years old and pertained to chemical weapons. At the same time as US government officials were routinely saying that about 20 nations had chemical weapons "capability," the Director of ACDA told the Senate Foreign Relations Committee on January 24, 1989, that apart from the US and the USSR "...no more than a handful, five or six" actually possessed a stockpile of chemical weapons." In the case of biological weapons, there are no equivalent statements in the public record. However in 1994, two senior US government officials stated in private meetings that no nation was then known to be producing and stockpiling BW agents. This was five years after US officials had publicly identified the ten nations having offensive biological weapons programs. In the years since 1994, official US statements have identified Iran as producing BW agents.

Accurate understanding has been further complicated, and continues to be so, in statements by official US government spokesmen in 1997 and 1998, that provide a single number grouping together nations with biological or chemical weapon programs. In October 1998, Richard Clarke continued the policy of US officials announcing confusing assessments, even including nuclear weapons in one single tally. In his remarks at the Washington Institute for Near East Policy, he observed that "Twenty-two countries, however, do possess them, if you consider biological weapons, chemical weapons, and nuclear weapons to be weapons of mass destruction."

On the other hand, statements of denial by various nations carry very little credibility in this field. The USSR did not admit to possessing chemical munitions until 1987. Indian officials denied for decades that their country possessed chemical munitions; they even claimed that their government had never so much as considered obtaining them. This past year, under the terms of being a signatory to the Chemical Weapons Convention, India declared its chemical weapons stocks. The government of Iraq lied for years about its production and possession of biological weapons stocks and delivery systems, and every indication is that they continue to lie about it.

As to how far offensive national BW programs have been carried out by different states, the relevant bits of information available in the US Non-Compliance documents and in the 1993 Russian Foreign Intelligence Report, as well as several estimates of my own, have been compiled in the summary shown in Table 2. It should be noted that US Department of Defense issues of <u>Proliferation: Threat and Response</u> do not identify specific BW agents produced by either Iran or North Korea. Testimony at the unclassified level by the Directors of the CIA and DIA has also omitted any reference to specific agents. Only the 1993 Russian FIS Report identified specific agents for North Korea. (It has proved impossible to corroborate various statements made in 1999 by US DOD officials, and in the Defense White Papers of South Korea and Japan, regarding numbers of different BW agents, or their identities, allegedly possessed by North Korea.)

Table 2. Biological Weapons: Offensive Programs, to the Degree Known

State	**Offensive R&D**	**Testing**	**Production**	**Stockpiling**	**Alleged Use**
Middle East					
Iraq	Yes	Yes	Yes	Yes	
Iran	Yes		Small		
Syria	Yes				
Egypt	Yes		In the past	In the past	
Libya	Yes		Small		
Israel	Yes	Probably	Probably (my estimate)		
Non-Middle East					
South Africa	In the past	?	In the past (small quantities)	In the past (small quantities)	In the past
Former Rhodesia	?	?	?	?	Yes, in the 1970s, wartime
North Korea	Yes	Yes (1993/FIS)	Yes (1993/FIS)		
USSR	Yes	Yes	Yes	In the past	Alleged; Afghanistan, glander, 1992
China	Yes	Yes	Yes	In the past	

Table 3

Of those countries that developed BW after World War II to the stage of weapons acquisition, virtually all either acquired all three categories of weapons of mass destruction (nuclear, chemical, and biological), or have acquired at least two categories and have made attempts to acquire the third. Thus:

- The United States, USSR, South Africa, and presumably China procured all three types.
- The United Kingdom and France procured nuclear and chemical weapons, and had offensive biological weapons programs.
- Iraq (prior to 1991) had chemical and biological weapons and was in advanced development of nuclear weapons.
- Israel has nuclear and chemical weapons, and an offensive BW program.
- Iran has chemical and biological weapons, and seeks nuclear weapons.
- Libya has chemical weapons, has sought nuclear weapons for decades, and is seeking biological weapons.
- Syria has chemical weapons and an offensive biological weapons program.
- North Korea has chemical weapons, has sought nuclear weapons, and (accepting the Russian assessment) apparently has biological weapons.
- India and Pakistan have nuclear weapons. India has chemical weapons; its biological weapons capabilities are unknown.

According to a statement by former CIA Director James Woolsey in 1994, nations developing and procuring BW have usually done so following their procurement of chemical weapons, and it has frequently been stated that various Arab states in the Middle East developed CW because Israel possessed nuclear weapons. There are no statements or analyses that have extended this rationale specifically to their development of biological weapons as well, although it is an easy, logical extension to make. Note Anthony Cordesman's phrase, "Nations that are interested in biological weapons are already interested because they offer an alternative to nuclear weapons...." It would not be altogether surprising if one learned that some government policy group in these countries that had considered or was urging the acquisition of nuclear weapons had spun off the suggestion to develop biological weapons. Nevertheless, nothing is publicly known regarding the policy decisions in these states regarding BW development.

As for the motives for national BW development programs, Table 3 indicates that every nation that has embarked on an offensive BW program has also sought or has produced either chemical weapons or nuclear weapons, or both.

There are several important additional points that should be noted in this section:

- None of the national BW programs cited above are new. They all date back about 15 years or more.
- One, South Africa s (which apparently was responsible for low-level BW use outside its own borders), was discontinued, as was the South African nuclear weapons program, immediately prior to the end of the apartheid government.

• There is no available evidence of the transfer of BW agent cultures from the former USSR or from Russian laboratories since 1992 to other countries of BW proliferation concern.

• There has also been minimal dispersion of researchers from former Soviet BW facilities to countries of concern. The total number of such individuals who emigrated from Russia (as of late 1997) was small, and of those, 90 percent became employed in the United States, Western Europe, or Israel. That leaves a very small number who moved to other countries, and some of those countries were also not of BW proliferation concern.

2. The Historical Record Regarding the Potential for State-Supported Terrorism with Biological Weapons

For over twenty years since its first appearance in 1979, the United States government has released an annual list of "State Sponsors of International Terrorism." This means that such states provide either some or all of the following to the very many groups that they support: training, sanctuary, documents, funding, explosives, or weapons. Of those states that have appeared on this list virtually year after year, no less than five also appear on the list of states that the US government charges have offensive biological weapons programs: Iraq, Iran, Libya, North Korea, and Syria.

This issue is germane because even those who admit that producing biological weapons might not be so simple a task for an isolated, non-national or terrorist group, the possibility is immediately raised that such a group could in theory obtain assistance, either in the form of training , technical assistance, or by direct transfer of a usable agent, from a state which does have a biological weapons capability. Nevertheless, there is no known evidence to date that such an event has ever happened, despite an extensive, decades-long record of very substantial assistance to literally dozens of different groups. Most government authorities, both US and other, tend to believe that if a state with biological weapons capability did want to make use of such weapons covertly, it would use its own and presumably better trained personnel to carry out the task and would not do so by transferring them to an external ad-hoc group. In 1996, the US Defense Intelligence Agency stated that: "Most of the state sponsors have chemical or biological or radioactive material in their stockpiles and therefore have the ability to provide such weapons to terrorists if they wish. However, we have no conclusive information that any sponsor has the intention to provide these weapons to terrorists."[1]

3. The Experience of the Use of Biological Weapons by Non-State Groups

This section is comprised of several parts, some continuing the essentially historical record of the material provided above, and others forming a transition to current assessments. These are:

a.) Databases on biological (and chemical) terrorism b.) A brief description of the efforts of the Aum Shinrikyo group in Japan to produce biological agents.

c.) The potential of terrorist use of biological weapons in the United States.

d.) The comparison of potential mass casualty biological events with current annual mortality in several public health categories.

A. Databases

Five extensive databases have now been developed and published since 1993. They were prepared by:

1.) Harvey McGeorge, in a DOD-contracted study, covering the years 1945 to 1994.[2]

2.) Ron Purver, at the Canadian Intelligence Service, covering the years 1945 to 1995.[3]

3.) Bruce Hoffman, at the RAND Corporation, covering the years 1900 to 1998.[4]

4.) Seth Carus, prepared for the National Defense University (US DOD), covering the years 1900 to 1999.[5]

5.) Amy Sands, at the Monterey Institute, Center for Non-Proliferation Studies, covering the years 1900 to 1999.[6]

All five are global surveys. Cumulatively, these databases contain nearly a thousand events in the twentieth century in a wide array of categories, extending from hoaxes, threats, consideration or discussion of use, purchase of materials, attacks on facilities, attempts to use, product tampering, and actual use. They are summarized in Table 4. All demonstrate the same result:

• There is an extremely low incidence of real biological (or chemical) events, in contrast to the number of recent hoaxes, the latter spawned by administration and media hype since 1996 concerning the prospective likelihood and dangers of such events.

• Those events that were real, and were actual examples of use, were overwhelmingly chemical, and even in that category, involved the use of easily available, off-the shelf, non-synthesized industrial products. Many of these were instances of personal murder, and not attempts at mass casualty use. The Sands/Monterey compilation indicated that exactly one person had been killed in the United States in the 100 years between 1900 and 2000 as a result of an act of biological or chemical terrorism.

• Excluding the preparation of ricin, a plant toxin which is relatively easy to prepare, there are only a few recorded instances in the years 1900 to 2000 of the preparation of biological pathogens in a private laboratory by a non-state actor.

Further, the 1999 publication of the book *Toxic Terror*, which contains a detailed examination of a dozen of the most well-known putative cases of the involvement of terrorist groups with chemical and biological agents demonstrated that exactly half of these were apocryphal.[7] This includes the notorious alleged German Red Army Faction “incident”, which for years authors such as Kupperman, Douglas, and others had referred to, allegedly relying on classified US government intelligence. The German security services (BND) had always claimed that the "case" was spurious, but its quiet suggestions to this effect had been disregarded.

It would be useful before going on to examine the case of the Aum group in Japan to look for a moment at the single instance of a mass casualty event that did take place in the United States using a biological agent. This was the use of Salmonella, placed on food in salad bars, by the Rajneesh group in The Dalles, Oregon, in 1984. This resulted in 751 recorded instances of illness, with no mortality. The group had discussed using a more serious pathogen, but decided against the risk of producing mortality, as their purpose was to incapacitate a large portion of the local population on the day of an election. The Salmonella was obtained from a type-culture collection, and the culturing work was carried out by a trained technician who belonged to the group. Given the calculated success of this event, and that its cause as an intentional act was not identified until long after the occurrence, it is nevertheless useful to compare the degree of deliberate injury that was caused by this act to the incidence of similar intestinal infections contracted by US tourists traveling in Mexico, the Middle East, Africa, and the Indian subcontinent <u>annually</u> since 1945. The rate must unquestionably be in the millions per year.

Table 4

Databases on Chemical and Biological Terrorism

1. <u>Harvey McGeorge</u>, 1994, chemical and biological, 201 to 244 instances:

Also includes:
- only threatened use
- actions against CB-related facilities
- actions limited to theft, purchase or fabrication of an agent, dissemination device, or related material

Results demonstrate a clear emphasis on low-tech, commonly available chemical, product-tampering, and poisoning

2. <u>Ron Purver</u>, 1995, chemical and biological, 92 instances (30 B and 62 C) in five categories

- threatened
- attempted to acquire
- acquired
- attempted to use
- actually used

(1998 and 1999 studies below demonstrate that many reported instances are apocryphal.)

3. <u>Bruce Hoffman</u>, Rand/Aberdeen database, begins with 1968

As of 1998, 8,000 terrorist events; only around 50 Weapons of Mass Destruction, including radiological

4. <u>Seth Carus</u> [NDU], August 1998, biological <u>only</u>, Bioterrorism and Biocrimes

Instances since 1900: used, acquired, attempted to acquire, considered acquisition, threatened to use.

45 use, but <u>only 5 since 1960</u> (<u>omits</u> most hoaxes, but does include some). Great majority of use for individual murder.

5. <u>Monterey Institute [Amy Sands]</u>, 1999

520 cases since 1900 to acquire or use C, B, R, and N (but includes <u>all</u> reported hoaxes, approximately 350 between 1997 and 1999).

- terrorist — 44 percent
- criminals — 56 percent (extortion, murder, other <u>non</u>-political)

B. The Effort of the Aum Shinrikyo group in Japan to Produce Biological Weapons Agents

In March 1995, members of a Japanese religious cult, the Aum Shinrikyo, were responsible for releasing the chemical agent Sarin in the Tokyo subway. They had produced the Sarin themselves, and their act killed thirteen people and injured several hundred (not 5,500, which was the number of people that arrived at hospitals.) They had also used Sarin undetected in June 1994 in another Japanese city, in an incident that produced seven deaths and injured 200. It was subsequently discovered that the group had attempted to produce biological agents between 1990 and 1994 and to disperse what they had produced on nine occasions in Tokyo and other nearby areas, to no effect.

The Tokyo subway event led to the US Senate Hearings in October 1995 held by the Committee on Government Operations, under Senators Roth and Nunn, which in turn catalyzed the train of decisions, programs and funding to counter the potential use of weapons of mass destruction in the United States. The public discussion in the United States for the past four years has, however, been overwhelmingly relegated to biological weapons, and bioterrorism. The experience of the Aum group in its efforts to produce biological agents is particularly important for several reasons, but it has been continually misinterpreted and misrepresented to mean precisely the opposite of what the experience demonstrated.[8]

First, as to what the group's capabilities were and what they did do:

- They had virtually unlimited funds to procure appropriate equipment, which they did through front companies they had established.
- They had adequate facilities, and four years in which to work undisturbed.
- They had about a dozen people with graduate training, not all in the appropriate disciplines, but with the kind of academic training which in theory should lead one to understand how to go about learning what one needs to know.
- They had attempted to buy assistance and technology in the USSR to aid their efforts to produce both chemical and biological weapons, and despite the expenditure of several million dollars, they appear to have come away empty-handed, certainly insofar as obtaining information concerning biological weapons. This last point is particularly important as one real-world reference point relating to the frequently expressed fear of the likely ease of procuring such information from unemployed or poorly-salaried former Soviet experts. (It can also be noted that there have been other even more striking failures in efforts to buy information from former Soviet BW scientists.)

Second, concerning what the Aum group was able to achieve or not achieve:

- They attempted to produce two biological agents, Clostridium botulinum (to obtain Botulinum toxin), and anthrax, both of which are constantly referred to as organisms which should be relatively simple to work with. They failed to produce either, and so of course their efforts to disperse these also failed. In fact, they could not have produced any infective anthrax because they had obtained a culture of a non-virulent, denatured vaccine strain of the organism.

- They did not have any Q-fever cultures, and therefore they were not "working with" that organism (contrary to various reports). They had attempted to purchase a Q-fever culture from a Japanese academic researcher, but were rebuffed, which is again of particular significance.
- They did not have samples of the Ebola virus, contrary to various reports, though it does appear that they had hoped to obtain them.
- Finally, they did not do any "genetic engineering," also contrary to some further misreporting.

There are two important points to be made. First, the Aum experience was a real, serious example, not the constant hypothetical evocations of unqualified, untrained terrorists being able to produce biological agents in kitchens, garages, bathtubs, and home beer brewery kits. Despite the expenditure of substantial time, effort, money and some requisite talent, their efforts totally failed. Second, it is my understanding that classified US government evaluations of the efforts of the Aum group to produce biological agents are the same as the information provided above. Despite this, no member of any agency of the US government has seen fit to provide a more proper public assessment of the lessons of this experience.[9]

C. The Potential of Terrorist Use of Biological Weapons in the United States

The discussion of this subject in the United States, beginning around 1996 following the disclosure of the 1990 to 1994 efforts by the Japanese Aum group to produce BW agents, and its use of the chemical agent Sarin in 1995, has been characterized by gross exaggeration, hype, misinformation, and, at times, even simple ignorance. It was overwhelmingly dominated by two clich s which were repeated *ad infinitum*: "It is not a matter of whether, just when," and "The nation will face within five years...." Five years have in fact now passed. Brian Jenkins (whose consulting group apparently staffed the July 2000 Report of the National Commission on Terrorism) characterized the discussion that ensued as fact-free analysis, and that in the absence of a validated threat, anxieties had been converted into conclusions. At a conference held by the Chemical and Biological Arms Control Institute on April 29-30, 1999 (the first of two two-day meetings under the rubric of "Bioterrorism in the United States: Calibrating the Threat"), Jenkins pointed out that when terrorist acts which could be relatively easily achieved, such as aircraft hijacking or product tampering first appeared as means used by terrorists, the rate of these events increased sharply year by year within five years. But the Aum experience has so far proved to be a single data point, and not the beginning of a trend.

Instead, what we have seen are many hundreds of hoaxes. Hoaxes are not BW, they are not "anthrax," and they are not "BW events." Nor are they terrorist consideration of the use of BW (or as phrased in the Defense Science Board Summer Study of 1997, demonstrations of "...the breadth of weaponry available" to terrorist groups), and they should not be counted in statistical compendia as such. A hoax is a <u>hoax</u>, and nothing else.

Two brief, but more expert assessments were provided to Congress early in 1999. John Lauder, Special Assistant to the Director of Central Intelligence for Proliferation, told the House Permanent Select Committee on Intelligence on March 3, 1999, that "...the preparation and effective use of BW by both potentially hostile states and by non-state actors, including terrorists, is harder than some popular literature seems to suggest." One should note that the statement included even "potentially hostile <u>states</u>," which would certainly make it even more difficult for "non-state actors. And Col. David Franz, then the Deputy Commander of the US Army s Medical Research and Materiel Command told the Senate Intelligence Committee that BW terrorism is <u>difficult</u> to carry out, and that it would require a "...large well-funded terrorist program or state sponsorship."

Estimates by official US government agencies of actual activities by terrorist groups to obtain biological weapons is contradictory. In February 1996, the US Defense Intelligence Agency responded to a question by the US Senate Select Committee on Intelligence by stating that, "We have no conclusive information that any of the terrorist organizations that we monitor are developing chemical, biological, or radiological weapons."[10] In the same year, the FBI Section Chief for Domestic Terrorism told Congress that, "to date, our investigations in the United States reveal no intelligence that rogue nations using terrorism, international terrorist groups, or domestic groups are planning to use these [nuclear, biological, or chemical] deadly weapons in the United States."[11] As an indication of how confusion gets introduced, even by the very same sources, on January 28, 1998, FBI Director Louis Freeh testified before Congress on threats to US national security. He noted that the FBI, which has jurisdiction over terrorism in the US, had opened over 100 cases in 1997 about the threat, development, or use of WMD, including biological agents, which was more than double the amount from the year before. Freeh noted that a significant fraction of the cases involved threats that had no basis in fact, and that most of the actual interest in biological threats seemed aimed against limited personal targets. He indicated, however, that up to approximately 30 investigations concerning WMD were continuing at the FBI. There never was a subsequent statement by any FBI official to clarify that all the remaining cases - as well as those in 1998 and 1999 - were <u>all</u> hoaxes.

Official statements made in 1999 were both variable and ambiguous. In June 1999, a "Fact Sheet" on "Chemical-Biological Warfare" prepared by the US Department of State opened with the following lines: "The Department of State has no information to indicate that there is a likelihood of use of chemical or biological agent release in the immediate future. The Department believes the risk of the use of chemical/biological warfare is remote, although it cannot be excluded." Two statements by CIA officials in 1999 and 2000 were different. In March 1999, Dr. John Lauder, of the US Central Intelligence Agency, stated that, "Beyond state actors, there are a number of terrorist groups seeking to develop or acquire BW capabilities," and reference was then made to the Osama bin Ladin network, for whom "acquire" rather than "develop" would probably be more appropriate.[12]

However, a statement by CIA Director George Tenet in March 2000 was actually somewhat of a retreat. He stated:

> ...we remain concerned that terrorist groups worldwide continue to explore how rapidly evolving and spreading technologies might enhance the lethality of their operations. Although terrorists we've preempted still appear to be relying on conventional weapons, we know that a number of these groups are seeking chemical, biological, radiological, or nuclear agents. We are aware of several instances in which terrorists have contemplated using these materials.
>
> Among them is Bin Ladin, who has shown a strong interest in chemical weapons. His operatives have trained to conduct attacks with toxic chemicals or biological toxins.[13]

Two points are notable: first that chemical, biological, nuclear and radiological were lumped together, and second that, "trained to conduct attacks" is not the same as Dr. Lauder s "develop or acquire BW capabilities." Tenet's reference to "biological toxins" also suggests ricin as the agent in question, for which there are other suggestions, together with efforts by the Bin Ladin network to obtain simple chemical agents rather than any effort by them to produce <u>either</u> chemical or biological agents.

There were repeated statements in 1999, most prominently in the September 1999 GAO report, *Combatting Terrorism: Need for Comprehensive Threat and Risk Assessment of Chemical and Biological Attacks*, that <u>no</u> threat analysis of this subject an examination of specific potential actors, their capabilities and intentions, and potential feasibilities — had ever been prepared inside the US government.[14] Instead, contractors had produced vulnerability analysis, scenarios of effects that would follow release of a BW agent. As indicated in the previous section, those systematic studies that have surveyed relevant events over the past 50 or 100 years uniformly predict that the most likely event will be, as they have in the past, the use of easily available off-the-shelf chemicals, individual poisoning, or the use of the most simply prepared toxins, such as ricin. A terrorist use of a BW agent is best characterized as an event of <u>extremely low</u> probability, which <u>might</u> — depending on the agent, its quality, and its means of dispersion produce high mortality (or economic damage if it is an anti-plant or anti-animal agent). Table 5 presents Brian Jenkins s April 1999 summary of the way the problem had been addressed in the previous several years. A very similar conclusion was reached by a US General Accounting Office report released in March 1999. It stated that

> ...plans developed by the Department of Health and Human Services for "medical consequence management" after a chemical or biological terrorist attack appear to

be "geared toward the worst-possible consequences from a public health perspective and do not match intelligence agencies judgments on the more likely biological and chemical agents a terrorist group or individual might use."

An essentially similar assessment was also reached by the Monterey group after their database study was completed.

> U.S. policy-makers and several outside analysts have predicted catastrophic consequences if a terrorist group or an individual — alone or with state sponsorship — ever mounts a major chemical or biological attack. These alarmist scenarios have been based on the potential vulnerability of U.S. urban centers to chemical or biological attack and the growing availability of relevant technology and materials. But these scenarios have not drawn on a careful assessment of terrorist motivations and patterns of behavior.
>
> With more than a hundred terrorist organizations active in the world today, the challenge is to identify groups or individuals who are both motivated *and* capable of employing chemical or biological agents against civilians. Yet instead of examining historical cases in which terrorists sought to acquire and use such agents, the Clinton administration, as well as many outside analysts, developed their threat assessments and response strategies in an empirical vacuum. Lacking solid data, they fell back on worst-case scenarios that may be remote from reality.
>
> The tendency of U.S. government officials to exaggerate the threat of chemical and biological terrorism has been reinforced by sensational reporting in the press and an obsessive fascination with catastrophic terrorism in Hollywood films, best-selling books, and other mainstay of pop culture.[15]

The past five years have been characterized, then, by:

- spurious statistics (hoaxes counted as "biological" events)
- unknowable predictions
- greatly exaggerated consequence estimates
- gross exaggeration of the feasibility of successfully producing biological agents by non-state actors, except in the case of recruitment of highly experienced professionals, for which there is no evidence to date
- the apparent continued absence of a thorough threat assessment, and thoughtless, ill-considered, counterproductive, and extravagant rhetoric

Perhaps the epitome of all this was the executive-level exercise in the spring of 1998 when "40 officials from more than a dozen federal agencies met secretly near the White House to play out what would happen if terrorists attacked the United States with a devastating new type of germ weapon".[16] The exercise was based on a scenario taken from a science-fiction thriller which had impressed the President: the postulated production of a viral chimera combining two viruses, smallpox and a hemorrhagic fever. But no such organism exists, and its fabrication would be a feat which virologists at USAMRIID, the US biological defense laboratories, believe is currently beyond the capability of the most advanced scientists and facilities to achieve, and perhaps is technically impossible.

Table 5

The Key Question: Does Catastrophic Terrorism (Incidents Involving WMD) Constitute a Clear and Present Danger?

A. An Informed Consensus?
1. Cannot assume that catastrophic CB terrorism is imminent.
2. Historical analysis provides no basis for forecasting catastrophic CB terrorism, however...
3. Analysis of current trends provides mixed picture.
4. With exception of OBL, not clear that any known group planning, but...
5. Perception of CB threat driven by vulnerabilities, changes in political and technological environments, consequences, and judgment of future generations.
6. We confront a diverse spectrum of potential actors, motives, purposes, capabilities, substances, targeting choices, levels of lethality.
7. Terrorist CB attacks causing catastrophic casualties likely to remain rare.
8. States or state-sponsored CBW represent potential threat especially in conflict with US.
9. CB hoaxes are increasing and will continue to be a problem.
10. Threat goes beyond casualties — enormous psychological impact, potential for economic warfare.

B. Risky Analysis in which Anxieties become Conclusions
1. Instead of assessing intentions and capabilities of an identified enemy, we begin with...
2. Identifying vulnerabilities, which are infinite...
3. Then positing a foe — they are legion — provided with a highly generalized motive...
4. To create a scenario focusing on worst cases...
5. Reifying a hypothetical scenario useful for planning purposes into an actual threat, considered inevitable, imminent, for which we are unprepared...
6. Demanding action (or future generations will judge us harshly) from which we might derive a deterrent effect.
7. Fact-free analysis lends itself to manipulation and other mischief.

C. Conclusions
1. Not just a matter of time before chem-bio terrorism occurs.
2. Hoaxes and threats more likely than use.
3. Chemical more likely than biological substances.
4. Small-scale more likely than large-scale attacks.
5. Crude dispersal in enclosed area most likely mode of attack.
6. CB terrorism is not about to become the car bomb of the 1990s.

D. A Comparative Perspective

Given the findings in the Sands-Monterey study that one single person died in the United States in the years 1900 to 1999 as a result of an act of biological or chemical terrorism, and the current discussion of biological agent terrorism as a potential mass casualty event, it is quite revealing to look at annual mortality in several public health sectors:

1.) Food-borne disease incidence in the USA (US/CDC, September-October 1999)
*76 million cases per year
*315,000 hospitalizations per year
*5,000 deaths per year

2.) Medical error mortality (US National Institute of Medicine, December 1999) *between 44,000 and 98,000 deaths per year

3.) Hospital-contracted infections (US/CDC, March 27, 2000)
*20,000 deaths per year
(Another, possibly overlapping estimate in the July 2000 WHO report on drug-resistant organisms, gave a US mortality of 14,000 per year).

4.) The 1993 cryptosporidium outbreak in Milwaukee, a result of water pollution, sickened 400,000 people.

5.) Air pollution in the US results in 50,000 deaths per year.

6.) Firearms result in 35,000 deaths per year, and $4 billion in medical expenses.

The sum of the first three categories alone results in between 69,000 and 123,000 deaths per year.

These figures certainly suggest a rather enormous misallocation of priorities: the US political system can absorb roughly 100,000 deaths per year in only three related public health categories — continuously, year after year, while appropriating hundreds of millions of dollars under the sudden presumption of a potential event of extremely low probability, the true likelihood of which is totally unknown. In discussions of the requirements for response to a "mass casualty biological terrorist event," analysts have defined "mass casualty" as anything between 100 and 1,000 individuals arriving at hospitals. That means that the US absorbs the mortality equivalent of between 100 and 1,000 "BW terrorist mass casualty" events per year without any qualm or problem. One might also note that individual diseases such as tuberculosis and malaria result in global mortalities of 2-3 million people each, per year.[17]

4. The Requirements to Produce Biological Agents by Non-State Groups

There are five essential requirements that must be mastered in order to produce biological agents:

- One must obtain the appropriate strain of the disease pathogen.
- One must know how to handle them correctly.
- One must know how to grow them in a way that will produce the appropriate characteristics.
- One must know how to store them, and to scale-up production properly.
- One must know how to disperse them properly.[18]

Four of the five requirements are in the portion frequently dismissed as "easy." Some experts do stress that the last step, aerosolization to the appropriate particle size for efficient inhalation infection, does present difficulties, while suggesting that the first four steps are simple. That is clearly not correct. Instead of dealing with this subject by abstract pronouncements, as is customary (and the more so the less initiated the commentator), it would be more useful to provide real examples from the experiences of several national biological weapons programs.

First, there is the problem of obtaining a strain of the organism in question that is useful for biological weapons purposes. Most natural forms of biological agents are not highly infectious, and it is not that easy to obtain the strains that are highly infectious. For example, in the course of the offensive phase of the US BW program, roughly 675 strains of Clostridium botulinum were gathered. More extensive laboratory research was carried out using about a dozen of these strains, and finally one strain that produced satisfactory titres of toxin regularly under production conditions was selected for weaponization purposes. Similarly for anthrax, the number of available strains is high and weaponization was carried out on only a few of these.

Secondly, even very practiced experts can run into significant problems. Dr. Jerzy Mierzejewski, the retired director of the Polish biological defense laboratories at Pulawy who spent his entire professional career working with Clostridium botulinum, plaintively expressed his persistent difficulties on working with the organism to participants at two NATO Advanced Research Workshops. One culture cycle would produce toxin that was lethal and a few months later the next would not, and so on over the years. Even variations in the growth parameters for non-pathogenic simulants could seriously degrade their intended performance. The British BW testing program used two common simulants, Bacillus globulii, and an E.Coli strain. It was discovered that even minor variations in their culturing parameters could seriously degrade their performance in aerosol dispersion tests.

As for more complicated integration of the entire process, another example is of value. Dr. William Patrick described the outcome of a study carried out recently at USAMRIID. A post-doctoral fellow was given the task of outlining how he would produce a mass casualty event using a designated organism that had been developed as a weapon in the pre-1969 US BW program — Tularemia. He was given one year in which to complete his assignment. When the year was up and he presented his project design, it was found that it included three errors that would have prevented the effort from being successful had it be carried out.[19] Quite unfortunately, Patrick has himself been responsible for publicly describing critical technical details which there is every reason to assume would not be known to uninitiated non-state or terrorist groups interested in producing or using biological agents.

At a meeting on "Bioterrorism in the United States" held on June 29-30 in Washington, DC, Jerome Hauer, former Director of the Office of Emergency Management for the City of New York, stressed that:

> Most of the agents are not readily available,
> Most of the agents are not easy to make, and
> Most of the agents are not easy to disperse.

Regarding aerosol dispersal in particular, Tucker and Sands write:

> The capability to disperse microbes and toxins over a wide area as an inhalable aerosol — the form best suited for inflicting mass casualties — requires a delivery system whose development would outstrip the technical capabilities of all but the most sophisticated terrorists. Not only is the dissemination process for biological agents inherently complex, requiring specialized equipment and expertise, but effective dispersal is easily disrupted by environmental and meteorological conditions.[20]

At the end of World War II, the US BW program at Fort Detrick comprised some 250 buildings and employed approximately 3,400 people. The number of person-years that were required to weaponize as "simple" an agent as botulinum toxin, together with access to highly qualified personnel, excellent facilities, and extensive testing ranges is quite significant.

Dr. Ken Alibek has given the figure of a combined total of 60,000 people (at all levels of technical expertise, from service personnel to scientists) in all of the multiple segments of the former USSR's BW program: Ministry of Defense, Biopreparat, Ministry of Agriculture, Ministry of Health and so on. Senior scientists may have accounted for less than 5 percent of this total, and in seminars, Dr. Alibek has stated that although there were many experts that knew the precise details of an individual stage of the research or production process, there were perhaps only 100 individuals who knew how to take a particular organism that the USSR had weaponized through all its stages from beginning to end in the production process.

The Iraqi BW program began in 1974 or earlier, and between 1979 and 1985 a large number of their BW research staff were sent overseas for advanced study and degrees because it was apparent that work was not progressing and that they were not sufficiently trained and qualified. When the 200-300 BW researchers went back to work, they were supported by a separate contingent of over 1,000 technical people in the Iraqi chemical weapons program who carried out the BW testing program. The Iraqi BW program consumed upwards of $100 million.

One only has to compare the above with some of the descriptions of the supposed ease in producing biological agents that have been common in recent years. One author wrote that, "manufacturing a lethal bacterial disease agent requires little more than chicken soup, a flat whiskey bottle, and an available source of seed culture."[21] Another wrote that producing biological weapons was, "...about as complicated as manufacturing beer and less dangerous than refining heroin."[22] In seminar presentations a few years ago, former CIA Director James Woolsey would claim that a B-plus high school chemistry student could produce biological agents, and at a January 2000 meeting described producing biological agents as being "about as difficult as producing beer." In her book, *The Ultimate Terrorist*, Jessica Stern quotes:

Kathleen Bailey [who], after interviewing professors, graduate students, and pharmaceutical manufacturers, concluded that several biologists with only $10,000 worth of equipment could produce a significant quantity of biological agent.[23]

One can also compare these rather common and gross exaggerations with the real-world experience of the Aum Shinrikyo group:

- They had appropriate equipment (even more than was necessary).
- They used commercial front companies to buy the equipment.
- They may have spent in the range of $10 million in their effort to produce biological agents.
- Several of the individuals involved had post-graduate degrees.
- They had gathered a research library.
- They had sufficient time — four years — for their attempts.
- They had attempted to purchase expertise in Russia and to obtain or purchase disease strains in Japan.

However, they failed in their efforts to produce either of two biological agents.

5. A Summary Comment: The Real Danger of Exaggeration

A 1947 policy guidance promulgated by the US Department of Defense read as follows:

> This policy governs public information on Biological Warfare, Radiological Warfare, and Chemical Warfare and is based on consideration of the characteristics of these agents: of their possible use in offense; of the problems of defense against such agents; of the integration of an information program on BW-RW-CW with both the United States foreign policy and with United States domestic affairs.
>
> It is necessary that the American people understand the nature and scope of BW-RW-CW so as:
>
> a.) To appreciate the actual dangers which might arise from the use of BW-RW-CW and to participate effectively in defense measures against them;
> b.) To dismiss exaggerated notions and fears of the threat of BW-RW-CW;
> c.) To support U.S. Government policies concerning them.
>
> **II**
>
> This information is specifically designed to:
>
> a.) Provide the American people with authoritative information concern ing the nature and scope of BW-RW-CW; with due regard for security reg ulations;
> b.) Give the public information which without intensifying anxiety undu ly will enable Americans to act with maximum effectiveness and dispatch

in the event of a BW-RW-CW attack, or threat of attack, against the United States by either secret or overt means;

. . . . .

Official information which reaches the American public should, whenever possible, try to allay exaggerated fear. Therefore:

a.) All information on BW-RW-CW should be designed to convey the impression that the United States must become prepared to deal with such weapons.
b.) Such information should be characterized by a tone of confidence and moderation;
c.) Indications of apprehension on the part of U.S. Government leaders should be avoided.....[24]

In contrast, Secretary of Defense William Cohen has made a practice of determined exaggeration and apprehension the core of the US government's current policy on public information regarding the potential of the use of biological weapons. On November 26, 1997, the *Washington Post* carried a contribution written by Secretary Cohen on its editorial page. Speaking of biological and chemical weapons, Secretary Cohen wrote that:

- "...terrorist groups and even religious cults will seek to wield disproportionate power by acquiring and using these weapons that can produce major casualties..."
- "We should expect more countries and terrorist groups to seek — and to use — such weapons"
- "We have begun to treat the threat of chemical and biological weapons use as a likely — and early — condition of warfare."
- "Most ominous among these threats is the movement of the frontline of the chemical and biological battlefield from foreign soil to the American homeland."

The sentences quoted, portions underlined for emphasis, are exaggerated, inflammatory, counterproductive, essentially incorrect, and even dangerous.

A week earlier, Secretary Cohen had dramatically placed a five-pound bag of sugar on the table during a Sunday morning network TV program and stated that if released in the air over Washington, DC, an equivalent amount of anthrax would kill half the city's population, that is, 300,000 people. In March 1998, four of the most qualified experts on anthrax serving in the US government published a paper in the *Archives of Internal Medicine* which used a different estimate: 112 pounds of anthrax released over a city of 500,000 people could kill up to 95,000 people, and possibly many fewer, depending on urban atmospheric conditions. That is certainly horrific enough, but Secretary of Defense Cohen's estimate was approximately 100 times higher. As for Secretary Cohen's sentences quoted above, first there was no evidence available to the US government in 1997 that supported them; second, they are dangerous because by trumpeting a perception of US national vulnerability to chemical and biological weapons — whether or not that is actually the case — they are likely to induce and to stimulate both the interest of other states and terrorists in such weapons. They suggest that chemical and biological weapons are desirable, that they will be used on the battlefield and by terrorist groups, and that US authorities expect that to happen. None of these possibilities is necessarily the most likely outcome, and the way in which one portrays them is in fact likely to affect what that outcome will be. It would not have been difficult to conceive of language that would rather have been designed to deter the interest of other states and non-state actors in both the development and the presumptive use of biological or chemical weapons. Such language would have stressed the defensive measures being undertaken by the US government, as well as the likely consequences to any state or non-state party that used BW. Regarding any state that should be found to have used biological weapons against the United States, either covertly or overtly, US deterrent capabilities are formidable. (One has only to recall the US response to its suspicions — possibly mistaken — that the Sudanese Al-Shifta facility was producing chemical agent precursors.)

It is notable that no other government apart from the United States — none of our European allies, most of whom maintain analytic and defensive BW research establishments (UK, Germany, France, the Netherlands, Norway, Sweden, among others) — assess the likelihood of a BW domestic terrorism threat as the US does, despite several years of US government efforts to get them to adopt a similar view point, or at the least, to profess a similar rhetoric. In the United States, however, official influence and funding largess have had a profound effect. Many pages could be filled with a record of the past five years of contracted studies, conferences, media reports, and fictional popularizations. The examples below are typical:

> U.S. policy-makers now say that the threat of biological or chemical attack against a major American city is a reality that must be taken into account — especially with the rise of extremist political and religious groups. That dire message is being sounded this week at Stanford University, where senior U.S. officials, academics and security analysts, as well as a former secretary of state, are meeting to debate the rising risk that biological and chemical warfare poses to the public...The conference at Stanford's Hoover Institution on War, Revolution and Peace sought to improve intelligence-sharing on developments in biological and chemical weaponry and on ways to prevent its use. Across the board, however, the message was the same: There is a real possibility of massive civilian casualties in the near future caused by a superplague, a new lethal gas, or even a sprinkling of genetic time bombs that no one has yet figured out how to stop.[25]

> Terrorists will likely attack the United States with the smallpox or anthrax viruses within the next five to 10 years, says an expert who warns the country is unpre-

> pared. “We are a long way away from being even modestly prepared,” D.A. Henderson, director of the Johns Hopkins Center for Civilian Biodefense Studies, said Friday at a conference on bioterrorism.[26]

The two-day conference was attended by more than 300 physicians, scientists, public officials, and law enforcement agents to discuss possible ways to respond in the event of an attack. Dr. Henderson had organized an analogous conference in 1998, with approximately 1,000 attendees. These more professional meetings, of which there were many others, vied with more popular fare for the general public, such as the notorious Ted Koppel series that lasted nearly a week, a CBS Evening News “Eye on America special report on the biological terrorist threat,”[27] and a steady stream of fictional dramatizations, such as one in which a female secret agent “learns her alma mater is a training school for female agents and will unleash a strain of smallpox.”[28]

At the same time, after nine years of preparatory meetings and negotiations having now taken place in Geneva, successive US administrations have shown much less interest in seeing the achievement of a strong Verification Protocol to the Biological and Toxin Weapons Convention than our European allies. The combination of the two US policy choices has focused far more attention on biological weapons than would ever otherwise have been the case. If anything, it is the combination of the enormous and overblown official US emphasis on a domestic bioterrorism threat, and the US government's neglect of biological weapon arms control that is likely to spur a wider international resurgence of interest in biological weapons.

Endnotes

1.) United States Senate, Select Committee on Intelligence, *Current and Projected National Security Threats to the United States and its Interests Abroad*, Hearings before the Select Committee on Intelligence of the United States Senate, One Hundred Fourth Congress, Second Session, on February 22, 1996 (Washington, DC: Government Printing Office, 1996).

2.) Harvey J. McGeorge, “Chemical and Biological Terrorism,” Briefing Document, Public Safety Group, Woodbridge, Virginia, April 1996. See also Harvey J. McGeorge, “Chemical and Biological Terrorism: Analyzing the Problem,” *The AS A [Applied Science & Analysis] Newsletter*, no. 42 (June 16, 1994), pp. 1, 13-14.

3.) Ron Purver, *Chemical and Biological Terrorism: The Threat According to the Open Literature* (Ottawa, Canada: Canadian Security Intelligence Service, June 1995).

4.) Bruce Hoffman, “The Debate over the Future Terrorist Use of Chemical, Biological, Radiological, and Nuclear Weapons,” pp. 207-224, in *Hype or Reality: The “New Terrorism”and Mass Casualty Attacks*, B. Roberts, ed. (Alexandria, Virginia: CBACI, 2000).

5.) W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century* (Washington, DC: National Defense University, August 1998).

6.) Jonathan B. Tucker and Amy Sands, “An Unlikely Threat, *Bulletin of the Atomic Scientists* 55:4 (July-August 1999), pp. 46-52.

7.) Jonathan Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge, Mass: Massachusetts Institute of Technology Press, 1999).

8.) A detailed description of the efforts of the Aum group to produce biological agents is now available in three publications by Milton Leitenberg;

—“The Experience of the Japanese Aum Shinrikyo Group and Biological Agents,” in *Hype or Reality, op. cit.*, pp. 159-172.

—“Aum Shinrikyo’s Efforts to Produce Biological Weapons: A Case Study in the Serial Propagation of Misinformation,” pp. 149-158, in Max Taylor and John Horgan, ed., *The Future of Terrorism* (London: Frank Cass, 2000).

—“Aum Shinrikyo s Efforts to Produce Biological Weapons: A Case Study in the Serial Propagation of Misinformation,” *Terrorism and Political Violence* [Special Issue on the Future of Terrorism] 11:4 (Winter 1999), 149-158.

9.) One should add an additional point as a result of the papers referred to directly above: all of the portrayals of the Aum and BW that derived their information from the Kaplan and Marshall book and the 1995 Sopko and Edelman Senate Committee report are therefore thoroughly in error. This includes the books by Tom Mangold and Jeff Goldberg (*Plague Wars*), Jessica Stern, and others.

10.) United States Senate, Select Committee on Intelligence, *Current and Projected National Security Threats to the United States, op. cit.,* p. 213.

11.) See testimony of John P. O'Neill, Supervisory Special Agent, Chief, Counterterrorism Section, Federal Bureau of Investigation, p. 236, in United States Senate, Committee on Governmental Affairs, *Global Proliferation of Weapons of Mass Destruction*, Part I (Washington, DC: Government Printing Office, 1996).

12.) John A. Lauder, "Statement by Special Assistant to the DCI for Nonproliferation," House Permanent Select Committee on Intelligence, March 3, 1999.

13.) George J. Tenet, "Statement by Director of Central Intelligence before the Senate Foreign Relations Committee, March 21, 2000."

14.) GAO, *Combatting Terrorism: Need for Comprehensive Threat and Risk Assessment of Chemical and Biological Attacks*, GAO/NSIAD-99-163, September 7, 1999.

15.) Tucker and Sands, "An Unlikely Threat," *op. cit.*, pp. 46-52.

16.) Judith Miller and William Broad, "Exercises Find U.S. Unable to Handle Germ War Threat," *New York Times*, April 26, 1998.

17.) A former US Department of State and CIA counterterrorism official responded to the recently released report of the National Commission on Terrorism by noting that "More Americans have died from scorpion bites than from foreign terrorist attacks over the past five years." Vernon Loeb, "Terrorism Panel Faulted for Exaggeration," Washington Post, June 23, 2000.

18.) Dr. David Franz modifies this categorization slightly. After requiring "intent" on the part of the perpetrator, he lists "Access, R&D, Scale-up, Production, and Weaponization" as required stages in the process. For "Classical Battlefield Agents," he indicates that four of these — R&D, Scale-up, Production, and Weaponization — are all "Necessary and Difficult." If "Highly Contagious Disease Agents were used, these four stages are listed as "Not Necessary," and if Foreign Animal Disease Agents" were to be used (against domestic animals, not as an anti-human disease agent), the process if shortened to "Access and Use." Dr. David Franz, "Biological Terrorism: Which Agents Should We Worry About and Plan For?" CBACI conference presentation, January 10, 2000.

19.) Dr. William Patrick, CBACI conference presentation, January 10, 2000.

20.) Tucker and Sands, "An Unlikely Threat," *op. cit.*, pp. 51.

21.) Edith Kermit Roosevelt, "Germ War," *International Combat Arms* (July 1986), pp. 38-42.

22.) Douglas and Livingstone, 1987, p. 23 [reference incomplete].

23.) Jessica Stern, *The Ultimate Terrorists*, Cambridge, Mass: Harvard University Press, 1999, p. 50.

Dr. Bailey, a Livermore Laboratory staffer and determined opponent of both BW and CW arms control treaties, repeated this statement in innumerable seminar lecture presentations during the mid-1990s, at times identifying the "graduate students" as University of Maryland undergraduate biology majors, and the "interviews" as carried out by telephone.

24.) "Public Information Policy on Biological Warfare, Radiological Warfare, and Chemical Warfare," SECRET, Department of Defense, 1947. [Declassified, April 6, 1992]

25.) "US Faces Rear Chemical," CNN/Reuters, November 17, 1998.

26.) "US Ripe for Anthrax Attack, Expert Warns," APB News/Associated Press, February 5, 2000. (Anthrax is, of course, not a virus.)

27.) CBS Evening News/Eye on America, February 7, 2000.

28.) "Secret Agent Man," UPN/WDCA TV, Washington, DC, March 14, 2000.

Averting the Hostile Exploitation of Biotechnology

Matthew Meselson

Every major technology -- metallurgy, explosives, internal combustion, aviation, electronics, nuclear energy -- has been intensively exploited, not only for peaceful purposes but also for hostile ones. Must this also happen with biotechnology, certain to be a dominant technology of the twenty-first century?

Such inevitability is assumed in "The Coming Explosion of Silent Weapons", by Commander Steven Rose (*Naval War College Review, Summer 1989*), an arresting article that won awards from the US Joint Chiefs of Staff and the Naval War College:

> The outlook for biological weapons is grimly interesting. Weaponeers have only just begun to explore the potential of the biotechnological revolution. It is sobering to realize that far more development lies ahead than behind.

If this prediction is correct, biotechnology will profoundly alter the nature of weaponry and the context within which it is employed. During World War II and the Cold War, the United States, the United Kingdom, and the Soviet Union developed and field-tested biological weapons designed to attack people and food crops over vast areas. During the century ahead, as our ability to modify fundamental life processes continues its rapid advance, we will be able not only to devise additional ways to destroy life but will also become able to manipulate it -- including the processes of cognition, development, reproduction, and inheritance. A world in which these capabilities are widely employed for hostile purposes would be a world in which the very nature of conflict had radically changed. Therein could lie unprecedented opportunities for violence, coercion, repression, or subjugation. Movement towards such a world would distort the accelerating revolution in biotechnology in ways that would vitiate its vast potential for beneficial application and could have inimical consequences for the course of civilization.

Is this what we are in for? Is Commander Rose right? Or will the factors that thus far have prevented the use of biological weapons survive and even be augmented in the coming age of biotechnology? After all, despite the fact that the technology of potentially devastating biological weapons has existed for decades and although stocks of such weapons were produced during the Cold War, their only use appears to have been that by the Imperial Japanese Army in Manchuria more than half a century ago.

A similar history of restraint can be traced for chemical weapons. Although massively used in World War I and stockpiled in great quantity during World War II and the Cold War, chemical weapons -- despite the hundreds of wars, insurgencies, and terrorist confrontations since their last large-scale employment more than 80 years ago -- have seldom been used since. Their use in Ethiopia, China, Yemen, and Vietnam, and against Iranian soldiers and Kurdish towns are among the few exceptions. Indications that trichothecene mycotoxins had been used in Laos and Cambodia in the 1970s and 1980s proved to be illusory.

Instead of the wave of chemical and biological terrorism some feared would follow the sarin gas attacks perpetrated by the Aum Shinrikyo cult in Japan in 1994 and 1995 or would be occasioned by the arrival of the new millennium, there has been only an epidemic of "biohoaxes" and several relatively minor "biocrimes", confined almost entirely to the US. Nothing has come to light that would contradict the 1996 assessment of the Federal Bureau of Investigation, reaffirmed in July 1999, that:

> Our investigations in the United States reveal no intelligence that state sponsors of terrorism, international terrorist groups, or domestic terrorist groups are currently planning to use these deadly weapons in the United States.

Continued surveillance to deter and forestall terrorist violence and contingency plans to limit and ameliorate the consequences if it should occur certainly merit the attention and resources of government. But sensationalist publicity is at odds with the historical record.

Whatever the reasons -- and several have been put forward -- the use of disease and poison as weapons has been extremely limited, despite the great number of conflicts that have occurred since the underlying technologies of the weapons became accessible. Human beings have exhibited a propensity for the use, even the veneration, of weapons that bludgeon, cut, or blast, but have generally shunned and reviled weapons that employ disease and poison. We may therefore ask if, contrary to the history of other major technologies, the hostile exploitation of biotechnology can be averted.

The factor that compels our attention to this question is the possibility that any major turn to the use of biotechnology for hostile purposes could have consequences qualitatively very different from those that have followed from the hostile exploitation of earlier technologies. Unlike the technologies of conventional or even nuclear weapons, biotechnology has the potential to place mass destructive capability in a multitude of hands and, in coming decades, to reach deeply into what we are, and how we regard ourselves. It should be evident that any intensive exploitation of biotechnology for hostile purposes could take humanity down a particularly undesirable path.

Whether this happens is likely to depend not so much on the activities of lone misanthropes, hate groups, cults, or even minor states, as on the policies and practices of the world's major powers.

In the United States, there was abrupt and remarkable change -- from nearly thirty years of being deeply engaged in the development, testing, and production of biological weapons to the dramatic and unconditional US renunciation of biological weapons declared by President Nixon in November 1969 and the US renunciation of toxins three months later. Today the former US offensive biological weapons program and the logic behind its abolition are largely forgotten, although there are valuable lessons to be learned from both.

During World War II, research, development, and pilot-scale production of biological weapons was centered at Fort (then Camp) Detrick, in Maryland. Large-scale production was planned to take place at a plant near Terre Haute, Indiana, built in 1944 for the production of anthrax spore slurry and its filling into bombs. Equipped with twelve 20,000-gallon fermentors, it was capable of producing fill for 500,000 British-designed 4-pound anthrax bombs a month. Although the United Kingdom had placed a large order for anthrax bombs in 1944 and the plant was ready to begin weapons production by the following summer, the war ended without it having done so.

Contrary to the view that biological weapons are easy to develop and produce, by the end of the war Fort Detrick comprised some 250 buildings and employed approximately 3,400 people, some engaged in defensive work but many in the development and pilot production of weapons. Several years after the end of the war, the Indiana plant was demilitarized and leased to industry for production of antibiotics. It was replaced by a more modern and flexible biological weapons production facility constructed at Pine Bluff Arsenal, in Arkansas, which began production late in 1954 and operated until 1969.

A major effort of the 1950s was encompassed under Project St. Jo, a program to develop and test anthrax bombs and delivery methods for possible wartime use against Soviet cities. In order to determine quantitative munitions requirements, 173 releases of noninfectious aerosols were secretly conducted in Minneapolis, St. Louis, and Winnipeg -- cities chosen to have the approximate range of conditions of climate, urban and industrial development, and topography that would be encountered in the major potential target cities of the USSR. The weapon to be used was a cluster bomb holding 536 biological bomblets, each containing 35 milliliters of anthrax spore slurry and a small explosive charge fuzed to detonate upon impact with the ground, thereby producing an infectious aerosol to be inhaled by persons downwind.

In later years, a strain of the bacterial pathogen of tularemia, less persistent and with an average human infectious dose more reliably known than that for anthrax spores, was standardized by the US military as a lethal biological agent. Other agents -- the bacteria of brucellosis, the rickettsia of Q-fever, and the virus of Venezuelan equine encephalomyelitis, all more incapacitating than lethal, as well as fungi for the destruction of rice and wheat crops -- were also introduced into the US biological weapons stockpile, along with improved biological bomblets for high-altitude delivery by strategic bombers and spray tanks for dissemination of biological agents by low-flying aircraft. According to published accounts, these developments culminated in a major series of biological weapons field tests using various animals as targets, conducted at sea in the South Pacific in 1968.

Soon after Richard Nixon became president, a comprehensive review was undertaken of US biological weapons programs and policies -- which had been unexamined and unanalyzed by policy makers for fifteen years. Each relevant government department and agency was instructed to present its evaluation of the arguments for and against each of several options, ranging from retention of the offensive BW program to its entire abolition. Following this review, the president announced that the United States would unilaterally and unconditionally renounce biological weapons. The US biological weapons stockpiles were destroyed and the facilities for developing and producing them were ordered dismantled or converted to peaceful uses. President Nixon pledged that the US biological program would be restricted to defensive purposes, strictly defined. He also declared that, after nearly 50 years of US recalcitrance, he would seek Senate agreement to US ratification of the 1925 Geneva Protocol prohibiting the use in war of chemical and biological weapons. In addition, he announced US support for an international treaty proposed by the United Kingdom, banning the development, production, and possession of biological weapons, leading to the Biological Weapons Convention (BWC) of 1972.

It is important to note that these US decisions went far beyond the mere cancellation of a program. They renounced, without prior conditions, even the option to have biological and toxin weapons. What was the underlying logic?

First, it had become evident through the results of the US biological weapons program that deliverable biological weapons could be produced that, although subject to substantial operational uncertainties, would be capable of killing people, livestock, and crops over large areas.

Second, it was realized that the US biological weapons program was pioneering a technology that, although by no means simple to bring into existence, could be duplicated by others with relative ease, enabling a large number of states to acquire the ability to threaten or carry out destruction on a scale that could otherwise be matched by only a few major powers. The US offensive program therefore risked creating additional threats to the nation with no compensating utility or benefit and would undermine prospects for combating the proliferation of biological weapons.

The clear policy implication, reinforced by widespread abhorrence for any use of disease as a weapon, was that the United States should convincingly renounce biological weapons and seek to strengthen international barriers to their development and acquisition. The US renunciation of biological weapons was seen as a major step away from a universal menace. As wisely expressed by President Nixon, "Mankind already carries in its own hands too many of the seeds of its own destruction."

The BWC entered into force in 1975 -- the first worldwide treaty to prohibit an entire class of weapons. The Convention now has 143 states parties, the most important holdouts being in the Middle East. Unlike the Chemical Weapons Convention (CWC) of 1993, it has no organization, no budget, no inspection provisions, and no built-in sanctions -- only an undertaking by its states' parties to never, in any circumstances, develop, produce, stockpile or otherwise acquire or retain:

> (1) Microbial or other biological agents or toxins, whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes;
> (2) Weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.

The significance of the BWC lies in its statement of a clear norm -- reinforced by international treaty -- prohibiting any exploitation by states of biological agents and toxins for hostile purposes. It is important to note that its prohibition of biological agents and toxins for all but peaceful purposes and its reference not only to armed conflict but, more generally, to hostile purposes make the BWC applicable not only to hostile purposes of a state directed against another state but also to hostile purposes of a state directed against its own citizens or anyone else. Thus, the BWC embodies an international norm and provides a legal bulwark against the exploitation of biological agents or toxins by states for hostile purposes whether in armed conflict or in any other circumstance.

While the United States renounced biological weapons and abided by the BWC, the Soviet Union did not. According to statements by officials of the former Soviet program, it was believed that the US renunciation was a hoax, intended to hide a secret offensive program. Aware of the post-war US biological weapons program and of the dynamic US lead in molecular biology and biotechnology, the Soviet Union continued and intensified its preparations to be able to employ biological weapons on a large scale.

An example was the standby facility built in the early 1980s for the production of anthrax bombs at Stepnogorsk, in what is now the independent republic of Kazakhstan. Recently dismantled in cooperation with Kazakhstan under the US Cooperative Threat Reduction Program, it was equipped with ten 20,000-liter fermentors, apparatus for the large-scale drying and milling of the agent to a fine powder, machines for filling it into bombs, and underground facilities for storage of filled munitions. According to its Cold War deputy director, the facility conducted numerous developmental and test runs but never produced a stockpile of anthrax weapons. Nevertheless, there is no doubt that its purpose was to provide a capability to commence production on short notice if ordered to do so.

Field testing of Soviet aircraft and missile delivery systems for biological agents was conducted on Vozrozhdeniye Island in the Aral Sea. In a 1998 interview with a Moscow newspaper, the general in charge of Russian biological defense is quoted as saying that activities at the test site in the 1970s and 1980s were "in direct violation of the anti-biological treaty."

The Russian Federation has done little to convince other nations that the military core of the Soviet biological weapons program has been dismantled. The former Soviet biological weapons facilities at Ekaterinburg, Sergiyev Posad, and Kirov remain closed to foreigners. The US-Russian-British discussions that had achieved agreement on the principle of reciprocal visits to each other’s military biological facilities as a means of resolving ambiguities have foundered and are in abeyance. Resolving the problem and establishing conditions that will allow the two nations to cooperate in fostering global compliance with the BWC will require that the matter be accorded high priority on the agenda of US-Russia dialog.

At present, we appear to be approaching a crossroads -- a time that will test whether biotechnology, like all major predecessor technologies, will come to be intensively exploited for hostile purposes or whether instead our species will find the collective wisdom to take a different course. An essential requirement is international agreement that biological and chemical weapons are categorically prohibited. With the BWC and the CWC both in force for a majority of states, including all the major powers -- and notwithstanding the importance of achieving full compliance and expanding the membership of both treaties still further -- the international norm of categorical prohibition is clearly established.

The CWC, now with 135 states parties, prohibits the development, production, acquisition, retention, transfer, and use of chemical weapons. Like the BWC, its prohibitions are purpose-based, so that a toxic chemical or precursor intended for peaceful purposes, so long as its type and quantity are consistent with such purposes, is not a chemical weapon within the meaning of the Convention. As with the BWC, this criterion for what is and what is not prohibited, termed the General Purpose Criterion, is intended both to avoid hampering legitimate activities and to help keep the Convention from becoming outmoded by technological change. Also like the BWC, the language of the CWC is applicable not only to prohibited weapons intended for use against another state but also to such weapons intended by a state for use against anyone.

The stringent verification provisions of the CWC, designed with the active participation of the chemical industry, require initial declaration of chemical weapons and chemical weapons production facilities and subsequent verification on-site of the correctness of the declarations. Declared chemical weapons and chemical weapons production facilities must be secured and are subject to routine inspection until they are destroyed and such destruction must be verified on-site. Facilities that produce more than designated amounts of certain chemicals deemed to be of particular importance to the objective of preventing diversion for chemical weapons purposes must be declared annually and are subject to inspection. Suspect sites, whether declared or not, are subject to short-notice challenge inspection under managed access procedures designed to protect legitimate confidential information and to avoid abuse. All inspections are conducted by experts of the Technical Secretariat of the Organization for the Prohibition of Chemical Weapons (OPCW), the international operating arm of the CWC headquartered in The Hague. In the three years since April 1997, when the CWC entered into force, there have been nearly 700 inspections at declared sites. These include 60 chemical weapons production facilities in nine states (China, France, India, Iran, Russia, the UK, the USA, and one other and the Aum facility in Japan) and 31 chemical weapons storage sites in four states (India, Russia, the USA, and one other), holding 8.4 million chemical munitions and bulk containers, most of them in Russia and the US.

In Geneva, the Ad Hoc Group of States Parties to the BWC is negotiating a protocol to strengthen the Convention, including measures for verification. There is general agreement that there should be an international operating organization similar to the Technical Secretariat of the OPCW and that there should be initial declarations of past offensive and defensive BW activities and of current biodefence programs and facilities, vaccine production facilities, maximum containment facilities, and work with listed agents. It is also generally agreed that there should be provision for challenge investigation at the request of a state party, including investigation on-site, of suspected breach of the Convention.

In order to encourage accuracy in declarations and to help deter prohibited activities from being conducted under the cover of otherwise legitimate facilities, some states believe that declared facilities should be subject to randomly-selected visits by the international inspectorate, using managed access procedures to protect confidential information, similar to those practiced under the CWC. Other states and certain pharmaceutical trade associations have so far opposed such on-site visits. Other important matters, including the scope and content of declarations, the procedures for clarifying ambiguities in declarations, the substantive and procedural requirements for initiating an investigation, measures for assistance and protection against biological weapons, measures of peaceful scientific and technological exchange, and provisions affecting international trade in biological agents and equipment also remain to be resolved and are the subject of intense negotiation.

What can international treaties like the CWC and a strengthened BWC accomplish? First, they define agreed upon norms, without which arms prohibitions cannot succeed. Second, their procedures for declarations and on-site visits, monitoring, and investigation, including challenge investigation, pose the threat of exposing noncompliance and coverup, creating a disincentive for potential violators and increasing the security of compliant states. Third, these same procedures have the potential to resolve unfounded suspicions and to counteract erroneous or mischievous allegations. Fourth, the legal obligations and national implementation measures of such treaties act to keep compliant states compliant, even when they may be tempted to encroach at the limits, or to ignore violations out of political expediency. Fifth, treaty-based regimes legitimate and facilitate international cooperation to encourage compliance and to take collective action against violators, thereby enhancing deterrence. And sixth, as membership in the treaty approaches universality and its prohibitions and obligations enter into international customary law, holdout states become conspicuously isolated and subject to penalty.

In sum, a robust arms prohibition regime like that of the CWC and the BWC strengthened by the kind of protocol that one may hope will emerge from the present negotiation serve both to insure vigilance and compliance by the majority who are guided by the norm and to enhance the deterrence of any who may be disposed to flout it.

The prohibitions embodied in the BWC and the CWC are directed primarily to the actions of states, not persons. Both conventions enjoin their states parties to take measures, in accordance with their constitutional processes, to insure compliance anywhere under their jurisdiction, including a provision in the CWC obliging its parties to enact domestic penal legislation to this effect and to extend it to cover prohibited acts by their own nationals wherever such acts are committed. Nevertheless, important as such domestic legal measures can be, neither the CWC nor the BWC seeks to incorporate its prohibitions into international criminal law, applicable to individuals whatever their nationality and wherever the offense was committed.

Recently, interest has developed in the possibility of enhancing the effectiveness of the BWC and the CWC by making acts prohibited to states also crimes under international law. A treaty to create such law has been drafted by the Harvard Sussex Program, in consultation with an international group of legal authorities (for the text of the draft treaty see CBW Conventions Bulletin for December 1998, available at<www.fas.harvard.edu/'hsp/>). It is patterned on existing international treaties that criminalize aircraft highjacking, theft of nuclear materials, torture, hostage taking, and other crimes that pose a threat to all or are especially heinous. Such treaties create no international tribunal; rather their provisions for adjudication, extradition, and international legal cooperation are aimed at providing enhanced jurisdiction to national courts, extending to specific offences committed anywhere by persons of any nationality. The proposed treaty would make it an offence for any person -- including government officials and leaders, commercial suppliers, weapons experts, and terrorists -- to order, direct, or knowingly render substantial assistance in the development, production, acquisition, or use of biological or chemical weapons. Any person, regardless of nationality, who commits any of the prohibited acts anywhere in the world would face the risk of prosecution or extradition should that person be found in a state that supports the proposed convention. Such individuals would be regarded as hostes humani generis -- enemies of all humanity.

International criminal law to hold individuals responsible would create a new dimension of constraint against biological and chemical weapons. The norm against using chemical and biological agents for hostile purposes would be strengthened, deterrence of potential offenders, both official and unofficial, would be enhanced, and international cooperation in suppressing the prohibited activities would be facilitated.

What we see here -- the non-use of biological and chemical weapons; the opprobrium in which they are generally held; the international treaties prohibiting their development, production, possession, and use; the mandatory declarations and on-site routine and challenge inspections under the CWC; the negotiations that may lead to strengthening the BWC with similar measures; and the possibility of an international convention to make biological and chemical weapons offenses crimes under international law, subject to universal jurisdiction and applicable even to leaders and heads of state -- suggests that it may be possible to reverse the usual course of things and, in the century ahead, avoid the hostile exploitation of biotechnology. Doing so, however, will require wider understanding that the problem of biological weapons rises above the security interests of individual states and poses an unprecedented challenge to all.

Mathew Meselson is the Thomas Dudley Cabot Professor of the National Sciences, Harvard University, and co-director of the Havard Sussex Program on CBW armament and arms limitation.

Chemical and Biological Weapon Terrorism: Assessing the challenges from sub-state proliferation

Jean Pascal Zanders, Ph.D.

Introduction

The Japanese apocalyptic religious sect Aum Shinrikyo released the nerve agent sarin in the Tokyo underground system on 20 March 1995. Thirteen people eventually died and more than 5500 were injured. This strike was the sect s third intentional and indiscriminate release of sarin within a year. In March 1994 Aum Shinrikyo tried to assassinate the leader of a rival religious sect, the Soka Gakkai, but failed as the spraying system mounted on a van malfunctioned and contaminated its operators. The second attempt occurred in the town of Matsumoto on 27 June 1994, resulting in seven deaths and 600 injured. While the improved spraying system functioned, the targets of the attack three judges who were expected to rule against the sect in a land dispute survived with relatively minor injuries as a consequence of a series of errors by the sect s strike team.[1]

Following these incidents terrorism was said to have made a qualitative leap: for the first time a terrorist organization had discharged a so-called weapon of mass destruction. While some analysts had predicted the inevitability of the development, many still have difficulties in understanding the purpose of terrorist organizations resorting to chemical and biological (CB) weapons. Part of the explanation is the focus on the potential consequences of such an attack: because of their classification as so-called weapons of mass destruction, which lumps them together with nuclear and radiological weapons, CB weapons are said to be able to produce huge numbers of casualties. The immensity of the envisaged consequences defies rational explanation of the political motives for the terrorist attack.

Much of the analysis of the threat of terrorism with CB weapons has so far been directed towards circumscribing the threat, profiling organizations likely to resort to such weapons and investigating the requirements for consequence management. However, once it has been determined that a particular group has developed an interest in chemical or biological weapons, its eventual acquisition and release of these weapons is virtually taken for granted. With nuclear weapons as the yardstick, CB weapons are seen as easy and cheap to obtain. This black box approach has diverted attention away from what is actually involved in the acquisition of chemical or biological weapons by a terrorist group.[2]

While only a few cases of terrorist attacks using CB weapons have been documented in detail, this paper nevertheless attempts to set up an analytical framework to describe the process of proliferation to sub-state actors. A distinction is first made between terrorism with CB materials and terrorism with chemical or biological weapons. Second, the paper then deconstructs the threat of terrorists using CB weapons and sketches the evolution of the overall threat with CB weapons since the 1991 Gulf War. Third, it applies the assimilation model for the demand-side study of CB weapon proliferation in states to sub-state actors. The assimilation model focusses on the way the political and military imperatives, as constrained by the state s material base, become reconciled with each other so that the weapon under consideration becomes an integral part of the mainstream military doctrine. It can be applied to non-state actors, because it focusses on the many thresholds which the promoters of the armament dynamic must overcome and the opportunity costs they are willing to pay to overcome these thresholds. With non-state entities, some thresholds identified for states will be virtually nonexistent, while other ones will feature much more prominently. The presence of certain thresholds and their respective height consequently typify the way in which a non-state actor can structure its armament dynamic. Based on these insights, the paper concludes that while the acquisition of CB weapons by terrorists is definitely feasible, such organizations nonetheless face enormous obstacles on the path to a CB weapon capability.[3] This decreases the likelihood of such events occurring. Moreover, if terrorists acquire such a capability it is highly probable that the quality of the agents will be well below that of similar agents in military arsenals. Fourth, from these insights the paper draws conclusions about the preparations to respond to a terrorist strike that utilizes CB weapons.

Agents of terror

To avoid muddling the discussion, an explicit distinction between terrorism with chemical and biological materials, on the one hand, and terrorism with chemical and biological weapons, on the other hand, has to be made. Terrorism with CB materials deals with the use of any toxic substance or pathogen in pursuit of certain goals. Terrorism with CB weapons refers to the use of warfare agents, that is a toxic chemical designed, developed and selected by the military to support certain missions laid out in the military doctrine of a state. This distinction highlights the deeper significance of the 1995 sarin attack in the Tokyo underground: for the first time a terrorist organization turned to a warfare agent.

Terrorism has been practised throughout history and in all types of civilization. Poisonous substances, whether animal, vegetable or mineral, have been used for political assassinations or sabotage. Such use was always limited, because only few people had access to the substances and possessed the learning to use them. Despite the risk of harsh punishments, the prospect of certain success attracted poisoners to the substances.[4] A qualitative change regarding the knowledge and accessibility to toxicants took place during the 19th century. With the development and rapid expansion of organic chemistry and the chemical industry the number of poisonous compounds increased significantly. The most common causes of poisoning are accidents, suicide or homicide. Poison appeared in the pre-World War I domestic law of several industrialized countries as part of the penal code or health, food, drugs and cosmetics acts. Greater scientific understanding of the propagation of infections contributed to the deliberate use of disease for sabotage. For instance, as part of a programme coordinated in Berlin during World War I German agents cultivated pathogens in the United States and tried to infect horses and livestock ready for shipment to the war theatres in Europe and the Middle East.[5]

Chemicals and pathogens were also used in World War II for assassinations and sabotage. On 27 May 1942 Reinhard Heydrich, Reichsprotektor of Bohemia and Moravia, was allegedly killed by a grenade charged with botulinus toxin supplied by Great Britain to Czech commandos.[6] Soviet agents reportedly had 9-mm pistol bullets containing 22 mg of aconitine for use against German administrative officials in occupied zones. The bullet produced a sure deadly effect even when it failed to hit a vital part of the body.[7] Polish and Soviet partisans were also reported to have used biological agents in sabotage or assassination operations against German troops.[8]

Since World War II poison weapons have been mostly associated with secret services. In September 1978 the Bulgarian secret police assassinated the exiled writer Georgi Markov with a pellet containing ricin. The toxin is said to have been supplied from the Soviet KGB-run Laboratory 12, which specialized in substances that could kill quickly, quietly and efficiently.[9] In September 1997 the Israeli secret service Mossad attempted to assassinate the head of the political bureau of the Palestinian militant Islamic organization Hamas, reportedly with a lethal dose of the synthetic opiate fentonyl.[10] The Truth and Reconciliation Commission produced evidence that South Africa s apartheid regime developed various contraptions charged with a poison or a biological agent for use against the black population as part of its chemical and biological warfare programme.[11]

Terrorist organizations on the whole have shown relatively little interest in CB materials. The 1995 survey on CB terrorism by Ron Purver lists over two dozen reported instances of terrorist use or threat of use of biological materials and a considerable number of threats and incidents with poisonous substances.[12] The cases range from apparently empty threats to reports of acquisition and actual discovery of possession.[13] Nevertheless, many of the listed cases could arguably be classified as attempts at homicide, suicide or criminal extortion motivated by financial rather than political gain. Other cases involved the intelligence services of certain countries, as mentioned above.

Common to most examples is the discriminate use of the poisonous agents. Humans were targeted individually; horses and livestock also had to be infected apiece. Even in those cases in which the assailant is never directly confronted with his victims e.g., the poisoning with mercury of exported Israeli citrus fruits in 1978 by a Palestinian terrorist organization or the lacing of foodstuffs in shops with toxicants[14] the physiological consequences were limited to the person ingesting the toxic substances. Another shared characteristic is the clear mission-oriented purpose of the attacks with CB materials. In no documented attack with non-warfare agents, whether successful or unsuccessful, were such agents used for their own sake. On the contrary, the goals to be achieved through the use of such agents were narrowly defined. This direct goal—instrument relationship may explain, in part, why no mass destruction resulted from these strikes.

The scientific and industrial developments of the 19th century also laid the foundations for chemical warfare in World War I and the military biological warfare programmes. A huge number of toxic compounds were investigated for their suitability as weapons. In the 20th century around 70 different chemicals were used or stockpiled as chemical warfare agents. Even fewer were standardized. The basic reason is that the selection of an agent represents a compromise:

- A presumptive agent must not only be highly toxic, but also "suitably highly toxic", so that it is not too difficult to handle.
- The substance must be capable of being stored for long periods in containers without degradation and without corroding the packaging material.
- It must be relatively resistant to atmospheric water and oxygen so that it does not lose effect when dispersed.
- It must also withstand the sheering forces created by the explosion, as well as heat when dispersed.[15]

Thus, for example, the US binary nerve agents were less pure than the unitary ones, but to the proponents of the programme in the 1980s the relative ease of production, storage and transportation, the increased safety for the troops handling the binary munitions, and the less complicated processes of demilitarization and destruction more than compensated for this loss of purity.

Moreover, the military had several types of agent at their disposal and, depending on the mission, were able to select them on the basis of volatility versus persistency and lethality versus incapacitation. Candidate biological warfare agents were similarly selected on the grounds of a compromise between pathogenicity, survivability after release and controllability. Military biological weapon programmes included lethal, incapacitating and anti-crop agents. This mission-oriented selection of chemical or biological warfare agents shaped the direct goal—instrument relationship.

Another common feature of the CB weapon programmes was that, especially after World War II, the final production phases (synthesis of the actual warfare agent, manufacture of delivery systems, weaponization, testing) were essentially conducted in facilities owned or controlled by government agencies. This limited the accessibility to these technologies. Furthermore, the public discourse regarding the necessity of chemical or biological warfare agents in the military arsenals was fundamentally different. While their casualty-producing qualities entered the discussions, the rationale for their acquisition was also based on tactical, strategic and geopolitical considerations. Such arguments included offsetting an adversary s numerical superiority in a particular domain; targeting rear areas, including population centres; economic warfare, including destruction of crops; deterrence; and their utility as bargaining chips at disarmament negotiations.

As a consequence of the way the military envisaged to use these agents, CB weapons were widely viewed as indiscriminate instruments of warfare. The user does not have full control over the agent after release into the atmosphere and, even in a tactical setting, the agent may spread far beyond the primary target area on the battlefield, affecting combatants and non-combatants alike.

The goal—instrument relationship for chemical or biological materials, on the one hand, and chemical or biological warfare agents, on the other hand, is markedly different. This is a direct consequence of the criteria underlying the selection of the agents. The compromises in function of military utility may therefore have been a disincentive for terrorist interest in warfare agents. While warfare agents can definitely be used for assassinations or sabotage, there is no immediate rationale available for their selection for these purposes. Moreover, the terrorist grouping would have to overcome the many technological difficulties involved in the manufacture, weaponization and dissemination of these agents. Aum Shinrikyo, of course, did precisely that, but it is also the only known organization to have attempted to acquire and use warfare agents on a large scale.[16] The current threat predictions particularly those involving mass casualties appear incommensurate with current reality. Before looking into the internal motivations for a terrorist organization to acquire CB weapons, it is therefore necessary to investigate whether the overall threat perception regarding CB weapons has, in fact, changed and, subsequently, been injected into the threat projections of terrorism.

Deconstructing the terrorist threat with CB weapons

Part of the problem of rationalizing the use of CB weapons for terrorist purposes lies in the qualification of CB weapons as weapons of mass destruction. This has two major implications. First, it draws the attention of the analyst away from the political motives for resorting to CB weapons and towards the consequences of such employment. As small quantities of toxic chemicals, pathogens and toxins are said to be able to produce massive casualties, prevention, emergency response and logistics become the prime focus of policy analysis. The immensity of the envisaged consequences, in turn, defies any rational explanation of the political motives for the terrorist act and reflects on the assessment of the rationality of the perpetrators. Second, the grouping of CB weapons with nuclear weapons into the category of weapons of mass destruction blurs the threat and consequence assessments for each individual class of non-conventional weaponry. The most plausible type of weapons to be used in a terrorist strike is mentally linked to the most destructive weapon category and vice versa. Chemical weapons are thus implicitly associated with the far greater destructive power of nuclear arms, and the nuclear threat is heightened because of the greater plausibility of terrorist organizations acquiring chemical weapons. Between these two extremes, biological weapons occupy the middle ground: they are easy to acquire and said to be able to produce mass casualties. For each of the three categories, the potentially most lethal agents are the ones considered. Furthermore, as Western analysts tend to use nuclear weapons as the yardstick to measure the complexity and cost of armament programmes, CB weapons are almost by definition easy and cheap to produce. This, too, affects assessments of the terrorist threat with CB weapons.

The focus on the consequences of a terrorist attack with CB weapons has another important implication: it affects a state s security deficit. A state always confronts a variety of security challenges. As it can never meet all security contingencies no matter what preparations it undertakes, a security deficit emerges. While the security deficit contains an objective component for instance, the differences in numbers and types of weapons deployed by two or more adversaries it is foremost an expression of the subjective appreciation of the threat(s). In the threat analysis of terrorism the objective component is by and large absent: new organizations can spring up at different times; their motivations and causes will differ; knowledge of the weaponry at their disposal is fragmentary at best; and the strikes can come without any warning, in any place and at any time. The only known factors of the security deficit are the state s own vulnerabilities. Consequently, they define the threat. The high probability of a terrorist strike with biological weapons is thus assessed on the basis of, for example, the limited understanding of the behaviour of pathogens under various environmental circumstances in built-up areas, the presence of essentially unprotected ventilation systems in modern buildings, the limited capability to detect these agents before people are harmed, or the lack of organizational preparedness to respond to the envisaged disaster. In this way, the terrorist threat with CB weapons rests on worst-case analyses of every conceivable scenario and developments in a wide variety of terrorist organizations, which are then amalgamated into a single threat projection. Little distinction is consequently made between what is conceivable or possible and what is likely in terms of the threat of a terrorist attack with CB weapons.

This sense of vulnerability has developed rapidly and its origins are complex. On 13 May 1991 then President George Bush declared that the United States would forswear the use of chemical weapons for any reason, including retaliation, against any state once the Chemical Weapons Convention (CWC) enters into force.[17] The announcement represented a major policy shift. The way in which the victory had been achieved against Iraq in 1991 was then seen to have greatly devalued the military utility of CW. The new weapon technologies had basically rendered chemical weapons obsolete.[18] The confidence of 1991 cannot contrast more starkly with today s extreme sense of vulnerability to CB weapon threats.

Several events have contributed to this development. The use of chemical weapons by Iraq against Iranian soldiers and its own Kurdish population in the 1980—88 war brought the issue of proliferation to the fore. Many companies in Western Europe and the United States had supplied Iraq with key technologies for large-scale production of advanced chemical warfare agents and delivery systems. The Soviet Union and its satellite states had trained the Iraqi military in the conduct of chemical warfare and sold large quantities of weaponry, some of which Iraqi engineers succeeded in converting into chemical weapon delivery vehicles (e.g., the al-Hussein ballistic missile). At the time chemical weapon armament programmes were also reported in some other countries in volatile regions (e.g., Libya and Syria). However, only following Iraq s defeat in the 1991 Gulf War did the world learn of the extent and advanced nature of Iraq s CB weapon programmes. Moreover, the great efforts the Iraqi leadership was undertaking to conceal components of these programmes from UNSCOM inspectors testified to the high value modern-day proliferators attach to CB weapons. In addition, in the years following the liberation of Kuwait many soldiers of the coalition forces suffered a variety of medical conditions, collectively known as the Gulf War Syndrome. The lack of conclusive evidence that low-level exposure to chemical or biological warfare agents may or may not have been a contributing factor increased the sense of helplessness in the face of such weapons. This sense of helplessness has been further heightened by the possibility that the medical pre-treatments to protect the soldiers from the effects of CB weapons might actually also be a cause of some of the conditions.

As the events in Kuwait unfolded, the bipolar world order was gradually giving way to a new multipolar international system. Many local and regional conflicts, which had been suppressed during the Cold War, flared up into open wars. The early enthusiasm for peacekeeping and peace enforcement in the wake of the victory in the Gulf War soon ebbed away as many of the conflicts proved intractable and led to relatively heavy casualties for the intervening forces. It also gradually dawned on policy makers and military planners that, as a consequence of proliferation, these troops may one day confront an adversary armed with chemical or biological weapons. Whatever the causes of the Gulf War Syndrome, the phenomenon highlighted many inadequacies in current CB weapon defence, detection, protection and prophylaxis. For forces unwilling to sustain high casualty rates (especially in view of the remarkably low number of casualties in Kuwait) asymmetrical warfare with CB weapons was suddenly perceived as able to defeat armed forces equipped with the most modern conventional weaponry.

Meanwhile, the international community was also moving rapidly to strengthen the regimes banning the possession and use of CB weapons. In January 1993 the CWC was opened for signature. States parties to the 1972 Biological and Toxin Weapons Convention (BTWC) began to consider verification and other measures to significantly strengthen the treaty. However, some events, in addition to the discoveries in Iraq and proliferation, raised questions about the value of the security offered by these treaties.

Russian President Boris Yeltsin all but admitted to an offensive Soviet biological weapon programme in violation of the BTWC in 1993. Serious concern continues to exist about Russia s compliance with the convention. Trilateral verification and transparency exercises by the three co-depositories of the BTWC (Russia, the United Kingdom and the United States) have come to a halt feeding suspicions of Russian non-compliance, and, recently, highly publicized accounts by a former ranking official in the Soviet biological weapon programme appear to confirm the worst fears.[19] Similar reports have emerged regarding the development of new chemical warfare agents.

Neither the agents nor their precursors are featured in the lists of chemicals in the CWC and may therefore escape detection under its routine reporting and inspection mechanisms.[20] The rapid deterioration of economic and social conditions in Russia increases the possibility of highly trained specialists with knowledge of chemical or biological weapon development and manufacture being enticed with financial incentives to countries suspected of seeking such weaponry. Low security at the various chemical weapon storage sites in Russia raise the possibility of theft.

The disarmament treaties themselves have an impact on the relative threat perception. After the entry into force of the BTWC in 1975 CW gradually became the greater threat; in the 1990s biological weapons are once again the larger threat as the CWC sets new standards for verifiability and enforceability. This perception is exacerbated by the concerns about the poor detection capabilities for biological warfare agents and the problems of consequence management if a release of biological weapons were to occur. Against the background of the debates on asymmetrical warfare, the CWC ban on in-kind deterrence or retaliation appears to hobble a state party. Yet the whole purpose of disarmament conventions such as the BTWC and the CWC is that the parties to them must seek ways of ensuring security by means other than those that are prohibited.[21] This was precisely the deeper sense in President Bush s declaration on 13 May 1991. In a different context, the CWC seems to contribute subtly to the focal shift towards the consequences of possible chemical weapon employment. The ban on the use and preparations for use has removed the tactical, strategic and geopolitical rationale for acquiring chemical weapons from current discussions, leaving the element of casualty production.

Parallel to this evolution of the CB weapon threat perception, the face of terrorism has also changed. A greater number of actors are resorting to such tactics. The terrorist attacks have become more lethal, resulting in higher casualty rates per incident and wholesale destruction (although these were entirely due to conventional attacks).[22] Instead of seeking publicity or furthering a distinct political cause, the new perpetrators of acts of terrorism seem to view the maximization of casualties as a goal in itself.[23] Particularly the religious groups associated with apocalyptic millenarianism, redemptive fanaticism or racist and ethnic hatred are said to find justification for their acts of violence in the higher authority of God.[24] Because of their respective belief systems, mass casualties are not an impediment to the furtherance of their goals. Although so far such groups have mostly carried out their indiscriminate attacks with conventional explosives, they are said to be more likely to cross the political and moral barriers to employing CB weapons.

Some events in the United States have significantly contributed to the new threat perception of terrorism. During the Clinton presidency the United States suffered the first large-scale, indiscriminate terrorist strikes on its own territory. The 1993 bombing of the World Trade Center in New York left 6 dead and around 1000 injured; the 1995 bombing of the Alfred Murrah Federal Building in Oklahoma City resulted in 168 fatalities and around 500 injured. Most importantly, the latter attack almost coincided with the release of the sarin nerve agent in Tokyo, creating a mental link between mass casualties and the release of chemical and biological warfare agents by terrorists.

The acquisition of CB weapons

To judge the likelihood of terrorist attacks with chemical or biological weapons a clear understanding of the weapon acquisition processes from the perspective of the demand side the terrorist organization is required. The demand side is often reduced to a listing and examination of motivations, such as the relative power and prestige the possession of non-conventional weapons confers to a non-state group and the difficulties of state retaliation against terrorist groups, because they know no territorial boundaries.[25] Such reasoning is based on a state-level analysis of nuclear weapon proliferation. It is far from established that these motivations play any significant role in the acquisition of CB weapons by states. For all its weaknesses, the 1925 Geneva Protocol, which bans the use in war of CB weapons, eroded the legitimacy of their procurement and possession considerably. Public acknowledgement of such armament programmes therefore required extensive justification. Consequently, most possessor states shroud their CB weapon programmes in extreme secrecy so that they cannot assert their relative power and prestige based on these arms.[26]

Viewed from the demand side, CB weapon proliferation occurs when a political entity a state, sub-state or transnational actor decides to acquire a CB weapon capability where such a capability does not yet exist provided this decision is followed by a CB weapon armament dynamic. The armament dynamic which the proliferator must initiate and sustain is the central part of the definition: proliferation is not an automatic process, which, once started, leads to eventual use. Reversals of the initial decision may occur at any stage as a consequence of, for instance, the impact of dissenting views or unsurmountable technical problems. In other words, CB weapon deproliferation occurs as soon as the political commitment to the initial decision ceases to be renewed or if the political entity explicitly reverses that decision (e.g., by unilaterally forswearing the weapons or joining a disarmament treaty).

The tension between proliferation and the constant pressures towards deproliferation is captured by the assimilation model of armament dynamics.[27] Assimilation is the process by which for a particular weapon, weapon system or arms category political and military imperatives, as constrained by the political entity s material base, become reconciled with each other so that the particular weapon, weapon system or arms category becomes an integral part of current mainstream military doctrine. Any weapon, weapon system or arms category must thus satisfy both political and military imperatives. This presupposes the existence of a dual decision-making track: one on which military appraisements are primordial, and another on which political considerations play the dominant role. The military track relates to those decisions taken by the military organization to effect the military facet of a political entity s security policy, including first and foremost the development and implementation of a doctrine. The planners take into account external factors (e.g., the changing threat) and internal ones (e.g., decision outputs from the political track). On the political track, overall policy decisions on security and budgetary allocations are taken. These decisions may relate to the formulation of a security policy by the highest political authorities, the budget process, the expression of institutional interests, bureaucratic rivalries, and so on. As the military and political tracks interact with each other, any decision or set of decisions not only influences future decisions on the same track, but also has ramifications for progress on the other. A considerable level of tension may exist between both tracks, especially if operators on one track make demands that are irreconcilable with the basic goals or premises of actors on the other track.

Any initial proposal for a particular type of weaponry envisages a particular end result. However, the weapon that is actually produced and deployed may differ significantly from the originally anticipated one. This variance between the original concept and the final product is the aggregate of all opportunity costs paid in the effort to achieve that original concept. The process involves many discrete minor and major decisions at the various stages of the armament dynamic. As the proposed weapon enters the decision process, it has to overcome multiple thresholds. These may involve a wide range of issues, including funding requirements, priority allocation of various resources to overcome technical difficulties, political opportunism, public opinion, environmental concerns, constraints from international humanitarian law and disarmament treaties, and so on. To overcome such a barrier an opportunity cost must be paid. It involves financial expenses as well as the expenditure of political capital to ensure the continuation of the programme at a particular stage. Different times and circumstances may thus result in different opportunity costs to be paid for similar decisions in a comparable phase of the armament dynamic. Decisions and conditions hampering the armament dynamic are just as crucial as those promoting it: they affect the outcome as a consequence of an increased variance between the original concept and the final product.

The nature of the thresholds is determined by intrinsic factors, which relate to the political entity s material base, and extrinsic ones, which refer to the domestic or international environment in which the weapon is conceived. The political entity s material base constitutes a particularly important independent variable affecting the decision process on both the political and military tracks. It consists of the political entity s physical base geographic location, territorial size, population, presence of natural resources, easy access to resources abroad, etc. as well as the level of education and scientific, technological and industrial development, economic strength, and so on. It thus involves factors which the decision makers can hardly, if at all, influence within the time frame of the armament dynamic under consideration. In other words, all other factors being equal, differences in the material base of any two political entities may account for different characteristics and results of the respective outputs.[28] The intrinsic and extrinsic elements may thus raise or lower the opportunity cost for crossing a particular hurdle. Ultimately, should the aggregate of opportunity costs be too high a price to pay for the political entity, the armament dynamic fails and is one of the possible causes of deproliferation.

The assimilation model views the material, political and societal constraints as obstacles which the decision makers must overcome if they wish to pursue the weapon programme and for which they are consequently prepared to pay certain opportunity costs. The opportunity of applying the assimilation model to proliferation follows from the extra attention paid to the deficiencies in the material base of the political entity. Elements, alone or combined, that may play a role in defining the threshold, which cuts through both the political and military tracks, are the political entity s scarcity of certain natural resources, lack of technical skills, an insufficiently advanced level of education, an inadequate research or industrial base, and the like. Barring abandonment of the entire project, the political leadership may try to develop the missing ingredients indigenously, seek them abroad or opt for a combination of both previous options. Given the probable time frame in which the armament programme has to be realized, importing the missing elements may be the only feasible and, in the short run, the cheapest alternative. Especially if the dearth occurs in the physical base of the political entity, importation may be the sole possibility. Importation of particular technologies, knowledge or materials is, consequently, one way of structuring the political entity s armament dynamic, albeit one which entails a sizeable opportunity cost.

The assimilation model is a heuristic device designed to study CB weapon armament programmes in countries of which limited information is available on decision-making processes and the way they structure armament programmes. The identification of the thresholds on the dual decision-making track and the assessment of how they may be overcome enables the study of demand-side of proliferation irrespective of the type of governance. The same methodology allows the application of the assimilation model to non-state actors, such as terrorist groups. The identity of the thresholds can be assumed to be equal for all political entities. However, the relative height of the thresholds will vary among these entities. Certain thresholds identified for states will consequently only play a minimal or no role in a terrorist organization, while other ones will have a far greater relative impact. For instance, the part of the dual decision-making track on which a political entity formulates its military doctrine may be argued to be non-existent for terrorist organizations. If this were the case, from the perspective of the assimilation model, it would mean that all relevant thresholds for the CB weapon armament dynamic in the terrorist organization are located on the political decision-making track. Nevertheless, such a group can be expected to have an idea, however vague, why it is seeking such weaponry. The assimilation model, as a heuristic device, suggests that incomplete or imprecise formulation of these goals increases the likelihood of the wrong choice of agents, inadequate dissemination devices and procedures, or outcomes far below theoretical expectations (although an aleatory combination of factors can never be excluded). The way the political and goal-related (i.e., for a state actor, the military) imperatives are reconciled with each other directly affects the goal—instrument relationship of the selected weapon.

The key parameters for terrorist organizations

The material base of a terrorist organization seeking chemical or biological weapons is a key determinant, because it consists of elements which the organization can only alter with great investment of resources or time (See figure). The physical base comprises elements that will determine whether the organization will be materially able to acquire CB weapons. Some elements (e.g., membership size, financial assets and possession of property and infrastructure) the organization can alter over time through targeted policies. Aum Shinrikyo attempted continuously to expand its membership and to extract the largest possible amount of wealth from its members, its members families and its sympathizers.[29] The transfer of property rights, including those of companies, was part of the initiation rites of novices. A terrorist group has less direct influence over other components of the physical base. Its geographical location and the type of culture in which it is embedded have a direct bearing on the nature of the organization and/or its success. Aum Shinrikyo enjoyed its greatest success in Japan, where, for example, alienated members of the intellectual stratum of society were receptive to mysticism, and in Russia, where many victims of the social disintegration were similarly seeking solace in various kinds of mysticism. In contrast, the sect was unsuccessful in the United States and Germany, despite some targeted efforts. Other important components of geographical location for Aum Shinrikyo included the overall level of scientific, technological and industrial development of the Japanese society, the tax exemptions granted to recognized religious organizations, which enabled Aum to amass its considerable assets, and the general hands-off attitude of the Japanese authorities towards religious organizations as a consequence of the religious persecutions before 1945. In other words, the terrorist organization feeds from the society that spawned it.

[Figure: SEE ATTACHED FILE]

The second component of the material base consists of the internal characteristics of the terrorist organization. The organization can relatively easily exploit, manipulate or develop certain of these characteristics in function of its goals. As noted earlier, its culture may be based on social ideology, apocalyptic or millenarian visions, racial superiority, ethnic-nationalism, religious fanaticism, and so on. In the quest for chemical or biological weapons the level of education and training of the members as well as the science and technology base they are able to set up become important factors. Aum Shinrikyo launched repeated recruitment drives to attract promising young scientists and people with other required skills from Japan s leading institutes.

These people were able to set up the programmes and build the necessary installations. An important weakness in the CB weapon programmes, however, was the reliance on relatively unskilled sect members for the operation and maintenance of the installations, which contributed to many accidents and leaks from them. Internal secrecy and dedication to the cause of Aum Shinrikyo in the selection of members to work on the CB weapon programmes were other contributing factors. Another negative factor on the operational side was Aum Shinrikyo s limited functional specialization. The people in charge of developing the agents were also responsible for developing the dissemination devices. They also executed the attacks and their lack of experience in operational planning contributed to the many mistakes and failures. The levels of economic and industrial development refer to the ways and means the organization as a whole is able to optimize its resources and manage the priority allocations in function of its goals.

The societal environment in which the terrorist organization evolves provides a second set of factors which influences the leadership in its choices regarding chemical or biological weapons. The tension between the organization s threat perceptions and the internal and external norms that govern its behaviour has a major bearing on how the organization will develop and on the security strategies (plans of action; self-protection) it will adopt.

A terrorist group arises as a consequence of the fundamental dissatisfaction of its members with certain (or all) aspects of societal organization. Inevitably, that society will pose a threat to the very existence of the terrorist group. The greater the existential threat to the organization, the greater the chance of its resorting to extreme measures. In fact, this is the shared feature between the Rajneesh cult[30] and Aum Shinrikyo: they both turned to the indiscriminate use of non-conventional means when public authorities threatened the continued functioning of the sects. There is, in addition, a subjective side to the threat perception. As an officially recognized religious organization, Aum Shinrikyo enjoyed considerable tolerance of its activities by the law enforcement agencies, despite many complaints by parents of under-aged sect members and people living near sect compounds, as well as indicators of the sect s involvement in murders. Isolation from the broader society was an effective way to hide its CB weapon-related activities, but also fermented paranoid projections of the threat to the sect posed by Japanese institutions and outside powers like the United States. The risk that the many, rather precise, apocalyptic predictions by the sect s leader, Shoko Asahara, might not be fulfilled provided another incentive to help events through chemical or biological weapons.

Norms are another major factor influencing the behaviour of the terrorist organization and hence its willingness to pursue CB weapons. Norms, however, form a complex aspect of social interaction and often do not manifest themselves in an absolute, positivist form. For instance, several authors have claimed that the release of sarin in the Tokyo underground weakened the norm against the use of chemical weapons or lowered the threshold for other groupings to resort to CB weapons. Such statements do not indicate for whom or in relation to whom the norm was weakened.

The norm against CB weapons has essentially always been one between territorial, sovereign states, that is between equal partners in the international system. In view of several gross violations of the constraints existing at the time of the violations (1899 Hague Declaration IV, 2 on projectiles containing asphyxiating gases; 1925 Geneva Protocol) and the unwillingness of the international community to uphold the norm in the light of ulterior geopolitical interests (e.g., 1936 war in Abyssinia; 1980—88 Gulf War; the failure to disarm Iraq despite an explicit UN Security Council resolution) it cannot be said that these norms have been particularly strong. The CWC offers a far stronger norm: not only use, but also possession of chemical weapons and all preparations for offensive chemical warfare are prohibited. The obligations are subject to international verification, and they are enforceable. The CWC obliges states parties to enact domestic penal legislation to ensure that none of its nationals, wherever that person may be, or those present on its territory undertake activities in contravention of the convention. In other words, since the Tokyo underground attack in March 1995, the norm against chemical weapons has definitely been strengthened and even extended to the sub-state level. Moreover, in the wake of the Aum Shinrikyo attack Japan has promulgated legislation criminalizing the production, possession and use of CW.[31] Many other states have also reviewed their existing laws to see whether an event such as the sarin attack is covered or have adopted explicit provisions to that effect in their CWC implementation legislation. The BTWC is, as noted earlier, far weaker in these respects than the CWC, but the norm should also be strengthened once the additional protocol, currently being negotiated in Geneva, enters into force. In addition, the UN General Assembly adopted the text of the International Convention for the Suppression of Terrorist Bombings on 9 January 1998.[32] Attacks fall within the scope of the convention if they are carried out with an explosive or other lethal device .[33] These include not only conventional explosives or other incendiary devices, but also toxic chemicals, biological agents or toxins or similar substances, and radiation or radioactive material.[34] This is the first time that CB weapons are explicitly mentioned in an international counterterrorism agreement.

In summary, since March 1995 there has been a formal strengthening of the norms against CB weapons for states and sub-state actors and in relation to other states and sub-state actors. However, in practice norms are never absolute and are always weighed against other norms and interests. Domestic enforcement, for instance, may encroach upon freedoms of speech, religion, organization, and so on. It will depend greatly on the maturity of the political and legal system whether a society can differentiate between fundamental rights and criminal activities prepared and executed under the cover of these fundamental rights.

There is, however, a different angle to this debate. One historical aspect of the development of the taboo against CB weapons, which is often overlooked, is that the civilization that acquired such a mode of warfare clearly understood the military advantage it had over the enemy.

It held a monopoly over the surrounding societies. Moral qualms about the application of noxious and poisonous agents in war were not a factor. Consequently, that civilization virtually never formulated legal or moral constraints against these weapons until the monopoly had disappeared or the military advantage had been balanced in an asymmetrical way. A similar sense of power over the Japanese society, derived from the possession of sarin, was present among the leadership of Aum Shinrikyo. Rather than representing an erosion of a taboo, which never existed for the cult, it accelerated the armament process and increased the internal pressures to demonstrate the possession of that power to the outside world. The apocalyptic visions of its leader provided the appropriate social discourse for the new technology within the religious community, but the new technology in turn also helped to determine the genesis of the apocalypse.

The question regarding to whom the norm is applied also hinges on the recognition of the other party as an equal partner. International norms and laws emerged in the Westphalian state system because the sovereign territorial states recognized each other as equal systemic units that could enforce the content of an international agreement within the territory of their jurisdiction.[35] In contrast, a political unit like a religious empire could not and cannot enter into such agreements. First, in its view sovereignty is derived directly from God and is therefore universal. Consequently, the religious political entity cannot tolerate a different source of sovereignty.[36] Second, membership in the entity does not depend on territorial location but on adherence to the faith. The rules, norms and values of the empire apply to all members of the faith wherever they may be and do not apply to non-members.[37] Regulations, such as the prohibition of poisoned weapons, governed the conduct of belligerents sharing the same faith, but these weapons were quite permissible against infidels. History is replete with such examples from all great religions.[38]

For terrorist organizations founded in religion, these insights have a double implication. First, the norms maintained by the grouping may differ significantly from those of the broader society. Internal or external constraints that could raise the thresholds for acquiring CB weapons on the political track of the assimilation model may therefore simply be non-existent and the success of the armament dynamic, if undertaken, may depend entirely on factors present in the material base. Second, because of their religious convictions the group members may differentiate themselves from the rest of society to such an extent that the elimination of non-members even on a large scale can easily be justified. This world view may remove any objection against CB weapon use. Indeed, it may be an important promoter of the armament dynamic in its own right.

The strength of norms is also directly linked to the nature of the threat. Sovereign states facing an existential threat or perception that they must meet every security contingency at every level (total reliance on self-help) are less likely to adhere to international norms limiting their options, and are more likely to invest heavily in arms buildups, including chemical or biological weapons, and to defect from international security regimes (like disarmament treaties) if their vital interests are at stake. International law recognizes this tension, for instance, through the inclusion of withdrawal clauses in international treaties. The International Court of Justice did not contradict this principle in its opinion regarding the legality of nuclear weapons of 8 July 1996: it could not conclude that nuclear weapon use was lawful or unlawful if the survival of the state in question was at stake, despite the potential for massive and indiscriminate destruction.[39] [Hence the smaller surface for norms than threat perception in the figure.] Translated to terrorist organizations, it raises the question of whether an existential threat, especially one which is gradually building up and which the group feels it cannot manage, contributes to the erosion of whatever norms the group might abide by. The Rajneesh cult decided on the dissemination of salmonella in salad bars precisely to avert such a situation. Aum Shinrikyo executed sarin attacks in the Tokyo underground to divert the attention of the police, which was poised to raid the sect s facilities, away from the cult.

If the leadership of a terrorist organization decides to embark on CB weapon armament programmes it will have to make some key decisions regarding the priority allocation of its resources. The decision and the nature of the programme will depend on the security strategies and the way the group is structured. For example, a loosely structured, amorphous grouping with little central guidance (e.g., many transient right-wing groups and militias in Europe and the United States, including the abortion clinic attackers and the Oklahoma City bombers)[40] or an organization structured in small cells for maximum security will find it much harder to set up an indigenous CB weapon armament programme than a vertically, highly integrated and ideologically uniform group, such as Aum Shinrikyo or the Rajneesh sect. On the other hand the organization will be constrained by its material base and will have to seek many, if not all ingredients and technologies from outside. The nature and size of these constraints determine the degree to which the group must rely on external sources for its technologies, commodities and expertise. For a terrorist organization this can be a formidable challenge. Contrary to a state actor, which can buy the technologies abroad and hire specialists, a terrorist organization must work in total secrecy because of the absence of a safe haven on the territory it occupies and the constant threat that law enforcement officials may raid the facilities. This means, for example, that the organization cannot hire a specialist or technician for a limited time to solve a certain problem, but must recruit him and convince him of the justness of its cause. This import dependency is also a function of the complexity of the weapon system the leadership has decided to acquire. With the key components in place, the armament dynamic can continue along the dual track until the desired weapon is achieved, whereby the decision makers must overcome the various thresholds and pay the various opportunity costs, while trying to keep the variance as small as possible. The actual chemical or biological weapon in the hands of the terrorist organization will reflect the aggregate opportunity cost paid along the way (e.g., in terms of the quality of the agent). If the aggregate opportunity cost is too high for the organization then the armament dynamic has failed (e.g., Aum Shinrikyo s botulinus toxin and anthrax programmes).

The influence of the various parameters can be illustrated when comparing Aum

Shinrikyo with the Rajneesh sect. The Rajneesh sect was responding to a rapidly evolving crisis that threatened its continued existence. The person in charge was a qualified nurse with sufficient skills to cultivate a pathogen, but not to set up a sophisticated biological weapon programme. Moreover, the cult had no time to develop its material base. The goal was limited in scope and time, namely influencing the outcome of local elections. Therefore, the sect could opt for an incapacitating rather than lethal agent, thereby narrowing the technical requirements for the laboratory. The choice for a Salmonella strain, which causes food poisoning, also simplified the dissemination as a liquid solution could be poured on the food in public places. In addition, this reduced the need for functional specialization in the sect. The straightforward goal—instrument relationship also meant that as soon as the sect realized that it would not attain the desired outcome, it terminated its programme.

Aum Shinrikyo s plans were far more ambitious: it sought to destabilize Japan and eventually take over all its governmental functions. To this end, the sect pursued a broad set of instruments, including conventional weapons, an earthquake machine, a laser gun, a nuclear device, as well as CB weapons. While many accounts of Aum Shinrikyo s activities have focussed narrowly on the CB weapon programmes, the important point for demand-side proliferation analysis is that the sect actively sought a broad range of weaponry. This had two major implications.

First, the element of priority resource allocation by the sect leadership became an important element in the CB weapon armament dynamic. The sect spread its huge financial assets and other resources over several weapon programmes as it tried to become self-sufficient in every area. It even opted to establish its own production line for the Kalashnikov AK—74 rifle instead of purchasing the required firearms. The black market in Russia, where Aum Shinrikyo had a large following and many regional centres, could have provided ample opportunities. Each programme placed increasing demands on manpower, the ability of the offices outside Japan to purchase the required technologies, and so on. Moreover, each programme created its own follow-on imperatives. The prospect of mass-produced assault rifles, for example, raised the issued of trained sect members to use these weapons and, in turn, placed fresh demands on the recruitment drive (e.g., to attract highly-trained military personnel as instructors). Had the sect concentrated its resources more on the CB weapon programmes, it might have achieved greater success in terms of creating a viable biological weapon or larger production batches of higher-quality chemical warfare agents. As it turned out, the sect had some success in few of its weapon programmes.

Second, there is no rationale for the CB weapon programmes without the other weapon programmes. Aum Shinrikyo s ultimate goals were the creation of Armageddon, the toppling of the Japanese government, the subjugation of the Japanese population, and, finally, the establishment of its own form of governance. CB weapons can conceivably only play a role (e.g., through the creation of mass panic and exposing the weaknesses of the authorities to protect the population) in the first three phases, but are insufficient in and of themselves. Any large-scale release of chemical or biological warfare agents in isolation would invite a massive response from the law enforcement authorities (as ultimately happened after the Tokyo underground attack), leading to the potential demise of the organization. In other words, it was impossible in practice for Aum Shinrikyo to concentrate its resources on CB weapons. In view of the grand strategy the leadership had to spread its large, but nonetheless limited resources over the various programmes. From the perspective of the CB weapon programmes, this imperative was reflected in the raised thresholds on the dual-decision making track, which contributed to the reduced quality and quantities of the chemical warfare agents and to the failures with respect to the biological warfare agents. In summary, the factors that contributed to the establishment of the CB weapon programmes were ultimately also responsible for the rather poor results.

Conclusions: Reconstructing the threat

A terrorist strike with chemical or biological weapons is definitely feasible. Aum Shinrikyo demonstrated as much in 1995. Nevertheless, the likelihood of such an event recurring must be judged on the basis of realistic and testable parameters. The single most important problem in such an undertaking is the uniqueness of the Japanese cult and the armament programmes it set up. In several instances it is difficult to judge whether certain elements are constants or variables (e.g., the question whether the cult was a phenomenon unique to Japan or whether it could also arise in a different type of society).

This paper has attempted to construct an analytical framework based on the assimilation model for studying the demand-side of the proliferation process in states. The key question is how does a proliferator structure its armament dynamic in order to acquire a chemical or biological warfare capability, that is, having chemical or biological weapons assimilated in mainstream military doctrine. The model focusses on the many thresholds to be crossed on the political and military decision-making tracks and on the wide range of opportunity costs that must be paid to overcome these obstacles so that, ultimately, the imperatives of the various actors involved in the armament process become reconciled with each other. These thresholds can be assumed to be identical for all countries. However, the height of the respective thresholds will vary between any two countries as a consequence of the differences in their respective material base. Ultimately, these factors combined will account for the different outputs (including failure of the armament dynamic) in these countries. The assimilation model can be similarly applied to the proliferation of chemical or biological weapons to sub-state actors. The main differences between a state and a sub-state actor are found in the makeup of the material base, which are reflected in the different heights of the thresholds. In order to be able to contrast two similar actors, this study has used the 1984 attempt at mass food poisoning by the Rajneesh cult, although the pathogen, Salmonella typhimurium, does not qualify as a warfare agent as defined in this paper. The comparison nevertheless revealed some interesting insights about the goal—instrument relationship.

Chemical and biological weapons only make sense in relationship to specified goals. To

Aum Shinrikyo they represented two possible avenues to the ultimate goal of destabilizing Japan and taking over the government. They were to be used in conjunction with other exotic or devastating weapons, as well as with ordinary conventional firearms. (Arguments such as ease of production or relative cheapness merely have a bearing on how certain thresholds are overcome in the pursuit of these goals. In the case of Aum Shinrikyo these factors were arguably of limited importance in view of the massive investments in the other weapon programmes. They may have played a role in the sequence in which the various armament programmes were launched.) Had the sect focussed exclusively on CB weapons, it would have probably solved the problems of viability of the chosen pathogens, large-scale production of chemical and biological warfare agents, and effective dissemination. However, such an exclusive focus would not have served the totality of the final goals. Consequently, the sect had to engage in the politics of priority allocation of resources and the CB weapon programmes had to compete with the other weapon projects. Many factors that increase the aggregate opportunity costs for weapon programmes in states, such as inter- and intra-service rivalry in the military, institutional and parochial interests, influence peddling, and so on, were also observable in Aum Shinrikyo. The outcome was many unresolved issues in the CB weapon programmes as well as in the other weapon projects.

The material base upon which Aum Shinrikyo could draw was huge and few other terrorist organizations will be able to match it. The cult s failures and difficulties are therefore significant for the threat assessment of terrorism with CB weapons. Variations in the composition of the material base have an immediate impact on the ability of an organization to successfully sustain a CB weapon armament dynamic. For instance, only a vertically organized, highly integrated and ideologically uniform group appears to have the capacity to set up and operate a large-volume production line for chemical or biological weapons in absolute secrecy. Religious sects, more than any other group, come to mind. This definitely reduces the number of candidates that could sustain such an armament programme.

The high technical hurdles ultimately limited the range and affected the quality of the warfare agents Aum Shinrikyo was able to develop. Military-grade warfare agents therefore are unlikely to constitute the main threat. As the 1995 sarin attack in the Tokyo underground suggests, a terrorist CB weapon attack may result in relatively few fatalities and most victims are likely to suffer short or low-level exposure to the chemical or biological warfare agents. The long-term effects of such exposure are still poorly understood as is evidenced by the ongoing debates surrounding the Gulf War Syndrome. Part of the resources to counter CB weapon terrorism should therefore be invested into researching the long-term consequences and treatment of such low-level exposures. Failure to do so can lead to demoralizing effects in the affected society and ultimately contribute to the end goals of the terrorists.

However, the constraints in the material base can lead to a low-volume, high-quality manufacture of chemical or biological warfare agents. Loosely structured or cell-based terrorist groups or even lone individuals can produce small quantities of such agents. While this broadens the possibility of these agents being used in terrorist attacks, the probability must nonetheless be linked to the goal—instrument relationship maintained by the actor. Indeed, despite the toxicity or pathogenicity of the agents, the small quantities are unlikely to result in mass casualties. Rather, these high-quality agents would be effective for targeting individuals or small groups. Such discriminate use of warfare agents, however, does not differ fundamentally from the more traditional use of chemical or biological materials. The question can thus be raised whether this development would fundamentally affect the threat assessments. Over the past decades various kinds of terrorist organizations and individuals have been known to be in the possession of extremely toxic substances, but until recently it did not affect the overall threat assessment of terrorism.

A related question is whether, bearing the goal—instrument relationship in mind, the use of warfare agents for individual assassinations does not constitute a case of technological overkill. Possibly, a technological imperative distorts the goal-instrument relationship, whereby, for instance, toxicity or pathogenicity become the prime criterion for selecting a warfare agent. Technological overkill characterized some of Aum Shinrikyo s assassination operations: VX was injected into two victims with syringes, VX and sarin were used in three attempts to murder a lawyer assisting members seeking to leave the sect[41] and phosgene was sprayed through the letterbox in a failed effort to silence a critical journalist.[42] The sect could have arguably resorted to more cost-effective instruments. Its interest in the potentially most lethal warfare agents was, of course, a function of its visions of Armageddon. The selection of sarin, VX and anthrax was also influenced by the intense media attention to the consequences of these agents during the 1990—91 Gulf War.[43] However, the cult did not have the mix of agents at its disposal to meet different types of contingencies (as it did not plan for them). It is not inconceivable that in this void the competition between the various departments of the sect led to lobbying efforts with Shoko Asahara to demonstrate the effectiveness of a particular weapon and contributed to the use of an overkill capacity.

The discussion so far has focussed on variations of some key parameters in the assimilation model with respect to a terrorist organization wishing to establish an indigenous CB weapon capability involving some of the most sophisticated warfare agents. The working hypothesis was the simple equation underlying most current consequence projections: increased toxicity or pathogenicity equals high casualties. The correlation, however, is far more complex and not necessarily positive. The assumed (military) grades of toxicity and pathogenicity in the threat projection are not easily attained by a terrorist organization in large production runs (around 7.5 litres of 30 per cent pure sarin was made for the Tokyo underground attack). The dissemination of these agents can easily lead to emergency contingencies for which there is little planning today.

Replacing consequence assessments with the goal—instrument relationship as point of departure for threat analysis reveals a different aspect, whose relevance may increase if terrorist organizations acquire greater sophistication and maturity with respect to CB weapons than Aum Shinrikyo. If the choice for a particular chemical or biological warfare agent by the military is a balance between potency and logistical considerations in function of operational requirements, the question can be asked why a terrorist organization would not seek a similar balance between its technical capabilities and type of CB weapons in function of its goals. This balance can be struck in two different ways. First, a terrorist group could decide on, for example, first-generation chemical warfare agents such as phosgene or hydrogen cyanide. Their manufacture is technologically less demanding than that of nerve agents and the ingredients for their production are widely available. The purchase of these ingredients would therefore not necessarily arouse suspicion. Second, over the decades the military have investigated and synthesized thousands of extremely toxic chemicals, but rejected most of them for weaponization.[44] The reasons why they were ultimately not incorporated into the arsenals may be of less relevance to a terrorist organization seeking a CB weapon capability. In other words, a terrorist organization can choose from a huge number of less-known toxic compounds in function of its technical capabilities and aims. The first responders to a CB weapon terrorist attack may, consequently, be confronted with the effects of totally unexpected agents, another possibility which can be easily overlooked in the preoccupation with the threat of so-called weapons of mass destruction.

Finally, the prime reasons for using CB weapons on the battlefield are not necessarily casualty production. Terrain denial, degradation of combat effectiveness by forcing the enemy to don protective clothing, degradation of the operability of facilities and equipment together with the imposition of the need for elaborate decontamination procedures, the causing of terror and psychological exhaustion, flushing out enemy troops from strongholds, incapacitation, crop destruction, and so on, are all major applications of CB weapons. Terrorists too are not always interested in creating large numbers of casualties. Very often they hit high value targets, such as train junctions, resulting in major disruptions. Relatively large sections of the population suffer the consequences. Persistent agents, e.g., mustard, could easily be used in this way. The release of an incapacitant, such as a potent lachrymator agent, into the air conditioning system of an airport can easily shut down all activities without causing a single permanent casualty. Opponents of genetically-engineered food could resort to anti-crop agents to destroy harvests without physically harming a person. In summary, from the angle of the goal—instrument relationship the variety of possible agents is enormous. The targets and effects would be limited, but, should the terrorist group so decide, the establishment of a domestic production capability for these agents would be less demanding on the material base of the organization.

Chemical and biological weapons have been the main consideration in the present paper, because they represent the new qualitative element in the terrorist threat. Toxicants and pathogens have been applied in assassinations and sabotage since time immemorial. The fact that today more people may have access to the knowledge and the technologies required to manipulate these agents can increase the quantitative dimension of the threat, but their use will not generally lead to mass casualties. CB weapons, in contrast, are by their very nature indiscriminate and some military-grade agents can, in theory, produce large numbers of fatalities and other casualties. Their insidiousness, moreover, makes them ideal instruments for terror and chaos. However, the processes to manufacture and disseminate them in sufficiently large quantities to obtain these effects are far more complex than those associated with other chemical and biological materials. Despite large investments, Aum Shinrikyo s CB weapon programmes continued to be plagued by considerable problems. The dependency on outside sources for equipment and compounds combined with the fact that such a CB weapon programme must be run in total illegality considerably complicates the quest for such weaponry. Contrary to widespread belief, the norms against the state and sub-state acquisition and use of CB weapons have been greatly strengthened. In addition, many sectors of society have acquired a greater awareness of the security risks involved in proliferation and will therefore be less likely to be unwitting partners in the acquisition of CB weapons by terrorists. These elements are and will remain major impediments to the widespread use of CB weapons for terrorist purposes.

Notes

Dr Jean Pascal Zanders assumed responsibility for the SIPRI Chemical and Biological Warfare Project in 1996 and is the series editor of the SIPRI Chemical & Biological Warfare Studies. He was previously Research Associate at the Centre for Peace and Security Studies at the Free University of Brussels. He is the author of the chapter "The destruction of old chemical munitions in Belgium" in the 1997 SIPRI volume The Challenge of Old Chemical Munitions and Toxic Armament Wastes, co-author of the SIPRI fact sheets The Chemical Weapons Convention (1997) and Iraq: The UNSCOM Experience (1998), and co-author of chapters in the SIPRI Yearbooks 1997, 1998 and 1999. He has also written extensively on regime formation and the implementation of the Chemical and Biological Weapons Conventions and on regional security in the Middle East with respect to chemical and biological weapons. He is the principal contributor to the educational module for the Internet on chemical and biological weapon non-proliferation.

This paper originally appeared in The Nonproliferation Review, vol. 6, no. 4 (Fall 1999) and is reproduced with permission from the Monterey Institute of International Studies.

---

1 Anthony T. Tu, paper delivered to Chem-Bio 98: Combating the Terrorist Threat , sponsored by Jane s Information Group, Washington, DC, 6—7 October 1998. David E. Kaplan and Andrew Marshall, The Cult at the End of the World: The Incredible Story of Aum (London: Arrow Books, 1996), p. 144.

2 A similar approach has been noted in chemical weapon proliferation analyses, whereby the debate conjures up a continuum starting with the transfers from industrialized countries to the proliferator, and ending with the latter s acquisition of a chemical weapon capability. The predetermined end of this linear presentation of the chemical weapon acquisition process was probable

or at least possible use. Jean Pascal Zanders, "Towards understanding chemical warfare weapons proliferation," Contemporary Security Policy, vol. 16, no. 1 (April 1995), pp. 102—103.

3 The paper deals exclusively with internal processes of CB weapon acquisition and therefore not with state-sponsored terrorism and the possibility that a state may supply chemical or biological warfare agents. Several contributions in Brad Roberts, ed., Terrorism with Chemical and Biological Weapons: Calibrating Risks and Responses (Alexandria, VA: Chemical and Biological Arms Control Institute, 1997) deal with this threat.

4 Lewin, L., Die Gifte in der Weltgeschichte [Poisons in world history] (Berlin: Verlag von Julius Springer, 1920), p. XIV. The author details many examples of poisoning for political purposes throughout his book.

5 Erhard Geissler, Biologische Waffen Nicht in Hitlers Arsenalen [Biological weapons Not in Hitler s arsenals], Studien zur Friedensforschung Band 13 (M nster: LIT Verlag, 1998), especially chapters 2 and 3. Mark Wheelis, "Biological sabotage in World War I," Erhard Geissler and John van Courtland Moon, eds., Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945, SIPRI Chemical & Biological Warfare Studies no. 18 (Oxford: Oxford University Press), 1999, pp. 35—62. Both studies are based on documents from German archives.

6 Robert Harris and Jeremy Paxman, A Higher Form of Killing ([No place given]: Triad Granada, 1983), pp. 88—94.

7 Walter Hirsch (Col. Dr.), Soviet BW and CW Preparations and Capabilities, 15 May 1951, pp. 505—6.

8 Valentin Bojtzov and Erhard Geissler, "Military Biology in the USSR, 1920—45," in Geissler and van Courtland Moon, eds., Biological and Toxin Weapons , p. 163. Harris and Paxman, A Higher Form of Killing, p. 89. Jan Nowak, Courier From Warsaw (Detroit: Wayne State University Press, 1982), p. 63.

9 Harris and Paxman, A Higher Form of Killing, pp. 197—98. Ken Alibek, Biohazard (London: Hutchinson, 1999), pp. 172—74.

10 Allan Cowell, "The daring attack that blew up in Israel s face," New York Times, October 15, 1997, p. A8.

11 "South Africa s chemical and biological warfare programme" in Truth and Reconciliation Commission, Final Report, presented to President Nelson Mandela on October 29 1998, Volume 2, Chapter 6. URL, <http://www.truth.org.za/final/2chap6c.htm>.

12 Ron Purver, Chemical and Biological Terrorism: The Threat According to the Open Literature (Canadian Security Intelligence Service: Ottawa, June 1995), URL <http://www.csis-scrs/gc/ca/eng/miscdocs/tabintre.html#preface>, chapters Biological Terrorism and Chemical Terrorism .

13 The recent spate of anthrax hoaxes in the United States has significantly increased the number of cases. For an overview, see W. Seth Carus, "Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century", Working Paper, Center for Counterproliferation Research, National Defense University, Washington, DC, August 1998 (March 1999 Revision).

14 Purver, Chemical and Biological Terrorism, chapter on Chemical Terrorism .

15 Chemical Weapons: Threat, Effects and Protection, FOA Briefing Book no. 16 (Sundbyberg, Sweden: Defence Research Establishment FOA, 1992), p. 20.

16 The other major case was the indiscriminate use of Salmonella typhimurium, a common

cause of food poisoning, by the Rajneesh religious cult in The Dalles, Oregon in September 1984. The direct motivation was to prevent the inhabitants from re-electing two commissioners of the Wasco County Court who were hostile to the sect. Between 1981, when the sect established its community in Oregon, and 1983 tensions rose sharply with the local population because the cult was seeking to aggressively overcome the stringent Oregonian land use laws, which constrained development in rural areas. The Wasco County Court, which had to issue the permits for many of the cult s plans, became a major impediment to the sect s ability to conduct its activities. Removal from office of the two commissioners most hostile to the sect through the manipulation of the electoral process in the autumn of 1984 thus became the principal goal. As part of the plot the sect attracted thousands of homeless people to its community who, because of the liberal voting registration laws, would be able to vote for candidates favoured by the sect. The use of the pathogen was intended to tip the electoral balance further in favour of the sect by incapacitating a large segment of the local population.
The cult also attempted to physically harm the commissioners. On 29 August, during a routine fact-finding visit to the Rajneesh community, the two commissioners hostile to the sect were served a glass of water contaminated with Salmonella typhimurium. Both judges became sick and one had to be hospitalized. It is unclear whether this act was to intimidate or assassinate the commissioners. Murder was not beyond the pale. In the planning stages of the plot to decrease voter turnout, sect leader Bhagwan Shree Rajneesh reportedly commented that it was best not to hurt people, but if a few died not to worry. It is also not clear whether the sect would have aborted their plan to infect the local population if one or both commissioners had died. Ultimately, 751 people became ill as a consequence of the restaurant contaminations in September. Despite the apparent effectiveness the cult did not conduct any follow-on attacks. As it realized in October that the plot would fail it gave up the attempts to take over the county. Carus, "Bioterrorism and Biocrimes", pp. 57—66.
Salmonella, however, is not normally considered as a military agent and has been included in some listings precisely as a consequence of the Rajneesh attack. James A. F. Compon, Military Chemical and Biological Agents (Caldwell, NJ, The Telford Press, 1987), p. 373. Salmonella has also been described as an unsophisticated agent . Edward M. Eitzen, Jr., "Use of Biological Weapons," in Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz, eds., Medical Aspects of Chemical and Biological Warfare (Washington, DC: Office of The Surgeon General, Department of the Army, 1997), p. 447. The report of the 13th session (January 4—22, 1999) of the Ad Hoc Group negotiating a protocol to the Biological and Toxin Weapons Convention in Geneva does not list the pathogen. Procedural Report of the Ad Hoc Group of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, document BWC/AD HOC GROUP/44 (Part 1), January 29, 1999, pp. 152—54.

17 "U.S. will forswear CW use once treaty is in force," USIS Presidential Text EUR102, US Embassy, Brussels, May 14, 1991.
18 Joseph Fitchett, "U.S. Gulf lesson: Toxic arms devalued," International Herald Tribune, May 15, 1991, pp. 1 and 2. Pierre Simonitsch, "USA zu vollst ndigem Verzicht auf chemische Waffen bereit" [USA prepared for total renunciation of chemical weapons], Frankfurter Rundschau, May 15, 1991.
19 Alibek, Biohazard. Ken Alibek also gave several widely reported testimonies to the US

Congress and is regularly interviewed by the international press.

20 Vil Mirzayanov and Lev Fyodorov, "A poisoned policy," Moscow News, no. 39 (September 27, 1992), p. 9. Vil Mirzayanov, "Poisons the treaty left out," Wall Street Journal Europe (May 25, 1994).

21 Previous agreements, such as the 1925 Geneva Protocol, were mere contracts. Technically they ceased to be binding as soon as they were broken by another party and were not binding as regards non-contracting parties. From the outset it was clear that states parties to the BTWC and CWC remain bound to the disarmament imperative irrespective of actions by other countries.

22 Peter Chalk, "The evolving dynamic of terrorism in the 1990s," Australian Journal of International Affairs, vol. 53, no. 2 (1999), p. 152.

23 Joseph F. Pilat, "Prospects for NBC terrorism after Tokyo," in Roberts, ed., Terrorism with Chemical and Biological Weapons, p. 5. Jerrold Post, presentation on countering terrorist groups, in Conference on Countering Biological Terrorism: Strategic Firepower in the Hands of Many? August 12—13, 1997, Proceedings report PIPS-97-2 (Arlington, Virginia: Potomac Institute for Policy Studies, 1997), pp. 38—39.

24 Kurt Schelter, "Antiterrorismuspolitik auf nationaler und internationaler Ebene" [Antiterrorism policy on national and international level], Sicherheit und Frieden, no. 4, 1997, p. 208. James K. Campbell, "Chemical and biological terrorism: Asymmetric warfare in the twenty-first century," in Gunnar Jervas, ed., NBC—Weapons and Terrorism (Stockholm: Swedish Defence Research Establishment, FOA, October 1998), pp. 27 and 38.

25 Campbell, ibid., p. 27.

26 For example, only after the 1980—88 Gulf War did Iraq admit to possessing CW, although several UN investigation reports had accused it of waging chemical warfare. It was not until April 1990 that the Iraqi leadership began referring to its chemical weapon arsenal as proof of its technological and military prowess. Jean Pascal Zanders, "The chemical threat in Iraq s motives for the Kuwait invasion," in Jean Pascal Zanders, ed., The 2nd Gulf War and the CBW Threat, Proceedings of the 3rd Annual Conference on Chemical Warfare, Vredesonderzoek, Special Issue (Brussels: Vrije Universiteit Brussel, November 1995), pp. 41—42. When India admitted to secretly possessing chemical weapons in its declaration under the CWC in 1997, it not only embarrassed the military establishment and diplomats, but also affected its leadership position on non-proliferation issues among the non-aligned countries.

27 Jean Pascal Zanders, "Tackling the demand side of chemical and biological weapon proliferation," in Dietrich Schroeer, ed., Technology Transfer (London: Ashgate Publishing Ltd, 1999), forthcoming. The assimilation model is explained with graphics in the Internet Educational Module on CBW Non-proliferation, created by the SIPRI CBW Project and the Centre for Peace and Security Studies of the Free University of Brussels, URL <http://cbw.sipri.se>.

28 For example, the United States and Iraq both developed binary CW. In the United States the binary concept was viewed as the answer to many safety, ecological, logistical and political objections to chemical weapons and its promoters were willing to accept a less pure nerve agent, which was produced inside the munition on the way to the target, than that in a unitary shell or bomb. In Iraq, the so-called binary agent consisted of a GB/GF (sarin/cyclohexylmethylphosphonofluoridate). Iraq is less sensitive to public objections.

29 The references to Aum Shinrikyo in this section are based on the analysis by Kaplan and Marshall, The Cult at the End of the World.

30 See note 16.

31 Richard Lloyd Parry, "Japanese shaken by new gas attack," The Independent (London), April 20, 1995, p. 12. T. R. Reid, "Gas fells 300 in new attack in Japan," International Herald Tribune, April 20, 1995, pp. 1, 6.

32 International Legal Materials, vol. 37, no. 2 (March 1998), pp. 249—260.

33 Terrorist Bombing Convention, Art. 2, para. 1.

34 Terrorist Bombing Convention, Art. 1, para. 3.

35 For example, the first known international agreement regarding the prohibition of the use of poison weapons was concluded in Strasbourg between France and the German Empire in 1675, 27 years after the Peace of Westphalia. Officers were to exemplary punish the person who possesses or uses such implements. Lewin, Die Gifte in der Weltgeschichte, p. 563.

36 This conflict of religious versus secular sovereignty was the source of the Thirty Years War (1616—48), which ended with the demise of the Holy Roman Empire. Many of the current internal conflicts in, for example, Iran and Israel are similarly rooted in the duality of religious versus secular sovereignty.

37 For instance, Jews maintained a sense of community despite almost 2000 years of diaspora.

38 For example, in his work published in the late Middle Ages Von allerlei Kriegsgewehr und Gesch tz (On types of gun and cannon) Wulff von Senftenberg expressed reservations about his own proposals for poisonous fumes if used against Christians, but had fewer misgivings regarding use against the godless Turks or other infidels. Julius Meyer, Der Gaskampf und die chemischen Kampfstoffe (Gas warfare and chemical warfare agents) (Leipzig: Verlag S. Hirzel, 1925), p. 277. Daniel Patrick Jones, "The role of chemists in research on war gases in the United States during World War I," Ph.D. diss., University of Wisconsin, 1969, p. 40.

39 Shannon Kile, "Nuclear arms control," SIPRI Yearbook 1997: Armaments, Disarmament and International Security (Oxford: Oxford University Press, 1996), pp. 391—92.

40 Chalk, "The evolving dynamic of terrorism in the 1990s," pp. 157—58.

41 Entry from "Database of Incidents Involving Sub-National Groups and Chemical Biological, Radiological, and Nuclear Materials 1900—Present," Monterey Institute of International Studies, 1999.

42 Another assassination operation involved the 1984 sarin release in Matsumoto in an attempt to kill three judges. Bad execution of the assault (the sect s science chief overslept, forcing last minute changes to the plans), problems with the dissemination device created panic in the strike team and made it flee leaving the sarin outlet open, and a sudden change in the wind direction were ultimately responsible for the several hundreds of casualties. Forty-four pounds of sarin had been manufactured in preparation of the attack, which is illustrative of the overkill approach.

43 Aum Shinrikyo appears to have had an exclusive interest in agents that were formerly in the US arsenal or which the USA considers to pose the gravest threat. Although the sect obtained the production plans for sarin from Russia, it does not seem to have developed an interest in warfare agents typically in the former Soviet arsenals (e.g., soman or isomers of VX). In view of its large operations in Russia, the training of sect members by Russian military personnel and the general opinion that expertise and technologies can easily be bought in Russia, this may appear remarkable.

44 For example, in the 1960s several lethal agents apparently reached advanced stage of development in the United States. A whole range of so-called E-agents (experimental agents) was studied at Edgewood Arsenal. One of them, EA 1356 or the 1356th Experimental Agent, was field

tested at the Dugway Proving Ground in 1969. SIPRI, Chemical and Biological Warfare Volume II: CB Weapons Today (Stockholm: Almqvist & Wiksell, 1973), p. 298.

The Infrastructure Web: A System for Distributed Monitoring and Management[1]

George Cybenko, Ph.D. and Guofei Jiang[2]

Abstract:

National-scale critical infrastructure protection depends on many processes: intelligence gathering, analysis, interdiction, detection, response and recovery, to name a few. These processes are typically carried out by different individuals, agencies and industry sectors. Many new threats to national infrastructure are arising from the complex couplings that exist between advanced information technologies (telecommunications and internet), physical components (utilities), human services (health, law enforcement, and emergency management) and commerce (financial services, and logistics). Those threats arise and evolve at a rate governed by human intelligence and innovation, on "internet time," so to speak. The processes for infrastructure protection must operate on the same time scale to be effective. To achieve this, a new approach to integrating, coordinating and managing infrastructure protection must be deployed. To this end, we describe the key ingredients of an *Infrastructure Web*. The Infrastructure Web is a web-like architecture for decentralized monitoring and managing critical national infrastructures.

1. Introduction

Modern threats to critical national infrastructure are evolving at the same rate as the technology on which that infrastructure is based. This is a key axiom of the work described in this paper. To illustrate the point, consider the following chronology of events related to the recent Distributed Denial of Service (DDOS)[1] attacks launched against major e-commerce companies.

Early summer of 1999	DDOS capabilities are demonstrated at a European hacker festival.
Late summer of 1999	First DDOS attacks at the University of Minnesota are detected and documented.
November 1999	A workshop on DDOS attacks and defense mechanisms is hosted by the Computer Emergency Response Team (CERT)[2], Carnegie Mellon University.
December 1999	Programs for detecting DDOS zombies are distributed.
February 2000	DDOS attacks are launched against major internet sites.

March 2000	The possibility of a DDOS-type attack against the 911 system is identified.
April 2000	DDOS-type attacks against the 911 system are suspected in Texas.
Sometime in the future	DDOS attacks within the financial sector, using automatically generated consumer trading, will be detected.

This chronology illustrates two major points:

a. The time intervals between when a new threat is identified, when it manifests itself, and when it is modified (mutated) into different forms are relatively short and appear to be shrinking;

b. Threats within one sector (telecommunications/internet) can easily spill over into other sectors such as human services (the 911 system) and the financial system.

To meet these challenges, we need to leverage modern information technologies and create an infrastructure protection process that can operate seamlessly at an accelerated time scale. Moreover, that process must be able to monitor and manage the complex interactions between infrastructure segments that are becoming the norm. This is especially important considering the fact that many recent attacks on national infrastructure have been credited to pranksters and individuals working alone or in small groups. We have not yet really seen what kinds of damage well-financed, coordinated, professional attacks are capable of creating.

Like the World Wide Web, the Infrastructure Web should have the following characteristics:

1.) It should be decentralized, asynchronous and redundant;
2.) New elements can be added to it or old elements can be removed from it by authorized personnel but without centralized control;
3.) It should be searchable and self-organizing;
4.) It should allow new services to be built easily on top of existing services;
5.) It should allow for multiple, redundant communication paths between entities.

Section 2 of this paper describes the various stages in the Critical Infrastructure Protection process today together with our vision for how those stages can be integrated. Special attention is given to infrastructure related to information technology, namely internet and telecommunications, but we indicate how the ideas can be generalized to other infrastructure segments.

Section 3 describes the conceptual organization of the Infrastructure Web that we are currently implementing. The functional operation is illustrated through some examples. Meanwhile section 3 also gives a brief technical description for how the Infrastructure Web can be implemented, using current computing and networking technologies.

Section 4 is a summary and proposal for near term work in this area.

2. The Infrastructure Protection Process

The emergency management, public health, and more recently, computer security communities have decomposed their management processes into smaller, logically-concise stages. For example, the DARPA Information Assurance program is using the three-stage Protect-Detect-React paradigm to organize work within that area [3]. Figure 2-1 shows the six stages we propose for Information Infrastructure Protection. These stages roughly correspond to stages used in other emergency management areas with different degrees of granularity perhaps. We briefly describe each stage and its relationships with other stages.

Figure 2-1: The Information Infrastructure Protection Process
[Figure: SEE ATTACHED FILE]

2.1 Intelligence

The first step in infrastructure management is intelligence gathering about emerging threats. This is typically done using human intelligence reporting, analysis of unusual incidents, and information harvesting from open sources such as the web and news sources. This is the early warning system that can identify new threats early in the process, before they manifest themselves in real attacks or disasters. Red teaming, namely the use of selected experts for scenario building and threat design for proactive analysis, is an important part of this stage. We include that in the human intelligence component.

Figure 2-1 identifies three sources of intelligence for early threat identification: incident analysis, human intelligence, and automated tools for harvesting and organizing information from open sources such as the web and newsgroups. In the information infrastructure protection problem, early evidence of threats is often proposed and discussed in such open sources. Such open sources are useful for human-initiated threats but not so useful perhaps for predicting complex interactions between infrastructure elements or natural events and design flaws. Human intelligence is more important for identifying those threats.

From the point of view of automating this stage of the process, automated incident report analysis and monitoring of open web- and internet-based sources are most promising. Several organizations already provide on-line access to incident reports and threat alerts (see http://www.cert.org for example), although those resources are not organized to allow powerful search capabilities through a database engine interface. Ideally, a new incident report could be quickly and automatically matched against an on-line database of previously seen threats and attacks to see if the threat is novel or known. Today, this stage of early warning is done by experts who rely on their own memories, networks of colleagues, and ad hoc searches of archives of previous attacks.

Automated monitoring of the web and various news groups for early threat identification is technically possible today [4], but not done to our knowledge. We are currently developing such a capability.

Figure 2-2: Early Threat Detection and Warning
[Figure: SEE ATTACHED FILE]

2.2 Threat Assessment

Once a new threat is identified, risk assessment and some sort of cost-benefit analysis[5][6] of responding to the threat must be performed. This stage requires some sort of epidemiological model of how an attack or failure based on the threat will manifest itself and how it will affect other infrastructure systems. Basically, the question is: what are its dynamics? Related to this of course are the costs associated with containment or interdiction versus the costs of an attack or failure based on that threat. As is often the case in defensive strategies, the cost of defense can be much higher than the cost of the attack, but that must be weighed against the social and human cost of major systems failures.

At present, our understanding of infrastructure epidemiology is very poor, at least in the open literature. The challenge here is to develop quantitative models of how vulnerabilities are distributed nationally or even globally, and how failures based on those vulnerabilities can cascade through the overall infrastructure.

Such analyses will probably have to rely on large-scale discrete event simulations given that closed-form solutions are highly unlikely. Government, industrial, and commercial task forces must be able to provide quick and reliable input into the vulnerability assessment process so that some form of realistic cost-benefit analysis can be performed in the threat assessment stage.

2.3 Interdiction

The interdiction stage of infrastructure protection attempts to proactively prevent or prohibit attacks or failures based on known threats. Virus scanners, software patches, and improved network designs and protocols are examples of interdiction in the information infrastructure segment. An important element of interdiction is the training of system operators and law enforcement personnel, especially at the state and local levels, because these communities are typically the first responders to attacks and failures.

These ingredients in the interdiction stage typically operate at different time scales. For example, the deployment of more robust and secure designs and protocols can take many years to permeate the infrastructure because of lock-in effects. On the other hand, software patches and virus scanning updates quite often occur on the time scale of weeks. The training of early responders such as system operators and law enforcement and emergency management personnel is problematic because of the huge demands on time and expertise in those sectors. The rate at which new threats and vulnerabilities are arising outstrips the ability of such personnel to attend training meetings and courses so that remotely accessible, distance training using networked interactive material is necessary. Cost-benefit analysis is essential to identify threats and vulnerabilities that are most likely to have high impact because existing time commitments and obligations preclude the ability of first responders to be prepared for all possible failures. This stage of the process must focus on interdiction in high-cost and/or high-probability events.

Figure 2-3: The Threat Assessment Stage

[Figure: SEE ATTACHED FILE]

2.4 Detection

The detection of actual failures or attacks is enabled by monitoring distributed sensors that are positioned throughout the infrastructure itself. Raw sensor data must be harvested, mined, correlated, and otherwise analyzed. Examples of such sensors include computer network monitors (based for example on SNMP agents or packet analyzers), public health records, medical laboratory results, environmental monitoring stations, financial market trend monitors, and so on. Human observations in the form of natural language reports are also relevant to this stage.

Whereas the Early Warning System part of the process is meant to anticipate attacks and failures through proactive intelligence gathering and analysis, this stage is meant to respond to mature attacks and imminent failures. Ideally, threat assessment and interdiction has prepared the community for these events but that may not always be the case.

The challenge in automating this stage of the process lies in flagging anomalous events without generating large numbers of false positives. This requires training an automated system on normal and known behaviors, and flagging behaviors that fall outside this regime. The technical challenge here is that many new behaviors emerge in the course of natural, non-threatening operating modes. Much work remains to be done in this area.

2.5 Response

Once an attack or failure has been detected, an appropriate response is required. We focus on law enforcement or internal auditing responses to information infrastructure events. A major challenge in responding to cybercrime and cyberterrorism attacks is identifying the source of the problem. This requires forensic techniques that allow building a trail of legal evidence for future investigation while respecting the privacy of third parties. These considerations require the ability to do fast and reliable upstream packet tracing, something that currently requires time-consuming and relatively slow operator intervention. Moreover, the fact that many internet links are now operating in the multiple megabit and even gigabit per second range, archiving network traffic for forensic analysis is a major technical challenge. Early work in this area is promising but much development remains to be done.

Another fundamental challenge in responding to infrastructure failures and attacks is that the very systems, namely the telecommunications networks, that responders will have to use to coordinate a response are themselves part of the infrastructure and highly vulnerable to failures. Any future infrastructure web architecture must provide for out-of-band and otherwise redundant communication capability.

This can be accomplished through the use of multiple communication channels based on different protocols implemented by different vendors so that a single vulnerability does not compromise the whole system. In this case, standardization is bad for survival and we need heterogeneous systems. Additional out-of-band communication capability can be achieved by radio and satellite networking, which is currently being investigated on several fronts.

Figure 2-4: Out-of-band and redundant communications channels
[Figure: SEE ATTACHED FILE]

2.6 Recovery

In the law enforcement arena, recovery from an attack or other criminal activity related to national infrastructure includes archiving non-reputable evidence without violating privacy laws and standards. Complete analysis of the incident is required to learn from it and to archive its characteristics in appropriate databases for future use in detection and training. Technical challenges here include training of first responders on the appropriate forensic techniques that accomplish these goals.

3. Architecture

The above section has discussed the various stages in the critical infrastructure protection process and our vision for how those stages can be integrated. So now the question is: how do we integrate and implement these stages and visions into a real monitoring and management system? In this section we are going to discuss the architecture of the Infrastructure Web that we are implementing and give a brief technical description of how the Infrastructure Web can be implemented by using current computing and networking technologies.

In our proposal, the national infrastructure web networks are built up with four types of basic distributed components: Directory service, Infrastructure server, Sensor web and Emergency information search server. All these distributed components are organized and integrated throughout the national wide networks with Sun s Jini system [7]. Jini is designed for deploying and using services in a network and enables the construction of dynamic, flexible, and robust systems from independent distributed components. A framework of the infrastructure web architecture is shown in Figure 3-1. With this kind of architecture, we believe that the infrastructure web system can be exploited as a platform to implement our distributed infrastructure assurance vision.

Figure 3-1: The architecture of the Infrastructure Web
[Figure: SEE ATTACHED FILE]

3.1 Infrastructure Server

In the infrastructure web system, one infrastructure network server represents one critical infrastructure in the physical world and the server s IP address is the unique identification for the infrastructure. Basically the infrastructure server will have a real time database, an XML-based web, a simulation model and possible other services that are running on some ports with the server s IP.

The database acquires real time data from the sensor web or other sources such as some host-based detection systems. These data consist of the infrastructure's security status, internal states, and so on. Some data will be displayed on the web real-time to show the infrastructure's current status, and some will be used in some simulations such as the threat assessment. Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) will be investigated to make the database access transparent.

By browsing the infrastructure's XML-based web, clients can check some security statuses and internal states of the infrastructure directly, F.g, the packet traffic throughput of an important LAN infrastructure. The relationships between related infrastructures will be described by XML s X-Link and X-Pointers [8]. A Resource Description Language (RDL) is created with XML DTDs and then the infrastructure's attributes can be well described in standard styles by RDL. Other web technologies such as Java applet and JavaScript will also be used to describe the infrastructures.

An essential part of the infrastructure servers consists of suitable analytical and simulation models of the infrastructures, together with a description of their behavior under dynamically changing interconnections. Just as we need to wire the pins of chips in a PCB (printed circuit board) design, by wiring infrastructure block's input-output, large-scale discrete-event simulations can be implemented for threat assessments. Moreover, like the PCB design tools, graphical simulation construction environments will also be investigated. We believe that with some adaptive learning technologies such as Neuro-computing and Evolution computing [9] some better planning, control, and coordinator strategies can be found in the simulations. These strategies and policies will be very helpful in making these infrastructures cooperate efficiently once a disaster or attack happens somewhere.

Some other services will also be implemented on the infrastructure server such as the host-based intrusion detection and early warning system described in section 2. The infrastructure server acts as a hosting platform for all these services.

3.2 Directory Service

Infrastructure web system has two-level directory services: local state level directory service and national level directory service. All these directory services will be implemented with Jini s lookup service. Infrastructures need to register themselves in the local Jini lookup services and all these local lookup services need to register themselves in the national level Jini lookup services.

Infrastructure's attributes are described in its registration, such as infrastructure's category and location, infrastructure servers IP and URL, proxy interface program for the database, and so on. Jini s attribute mechanisms support both type-based and content-based search styles and make searching for particular attributes simple, quick, and effective.

Jini system has five basic concepts: Discovery, Lookup, Leasing, Remote Events, and Transactions. All of Jini s ability to support spontaneously created, self-healing communities of distributed components is based on these concepts, and further, Java s Remote Method Invocation (RMI) and Object serialization [10] techniques make the implementations of these concepts available. The infrastructure web system is organized and integrated with Jini system and it inherits these concept advantage s from Jini. Fox example, with Jini s leasing concept, all infrastructures need to sign a lease with the lookup service in the registrations. Once the leasing time expires, the infrastructure will automatically be removed from the lookup service. In this way, Jini lookup service has a self-healing ability for its directory management and clients will not get the outdated or non-existent infrastructures information. Moreover, with the remote events concept, the relationship between related infrastructures can be better described. For example, infrastructure #1 can tell its related infrastructure #2 what kind statuses of infrastructure #2 it cares about. Once something happens to these statuses of infrastructure #2, just like a local event, infrastructure #1 will be automatically notified by the remote events from infrastructure #2. In this way, geographically distributed infrastructures can cooperate efficiently to detect, respond to and recover from the possible intrusion and attack.

Based on these Jini s concepts, we believe that the infrastructure web can be easily implemented to have the required characteristics that are proposed in section 1.

3.3 Sensor Web

The ability to monitor and detect stimuli or states of distributed infrastructures is another essential part of our system. In the analysis and detection of DDoS attacks, an analyst or upstream tracing system needs not only the packet log files from the local machines, but also those from some remote routers or firewalls. So here our sensor web system is actually a large-scale Distributed Smart Sensor Network (DSSN) that collects distributed sensor information both from intelligent software sensors and smart hardware sensors. Just like the infrastructure, Sensor web registers its sensors in the Directory Service and all these sensors can offer distributed data sensing services. Examples of sensors include computer network monitors (based for example on SNMP agents or packet analyzers), public health records, medical laboratory results, environmental monitoring stations, financial market trend monitors, and so on. Human observations in the form of natural language reports are also relevant to this stage.

The advances in measurement devices have reduced cost to the point that it is now viable to develop large-scale distributed sensing systems. Meanwhile, the advances in processor technology allow for relatively low-cost, low power, compact distributed processing integrated within these sensor devices, commonly referred to as smart sensors. Intelligent or smart sensors capable of parsing and filtering to leave only the necessary or desired information, allow for efficient use of memory, precious wireless bandwidth, and battery power needed for the transfer of sensor information.

Before sending the sensor information to the related infrastructures, sensor web system will preprocess the data from the distributed sensors using methods such as data filtering, data fusion, and data mining. More information about our distributed sensor web systems can be found in [11].

3.4 Emergency Information Search

Once some infrastructure fails or is attacked intentionally, there needs to be very quick response to and recovery of the infrastructure's damage. Some alternative infrastructures should be adjusted to cover the damage, and the possible related infrastructure's statuses should be checked to help the coordinators make correct decisions. Unfortunately, until now there have been no emergency information search and response systems of this kind available. Infrastructure web has a national wide Jini directory service and all the critical infrastructures register themselves in that directory service. We believe that the infrastructure web system can play the role of searching and offering emergency information during all of the proposed protection processes.

Just like the 911 telephone emergency systems, the emergency information server should have a special and well-known domain name and the emergency query forms should be well formatted. After clients submit the query, the HTTP server will transfer the query data to the CGI or Java Servlet programs. These programs will process the query data and submit a formatted attributes template to the Jini lookup services. Then Jini systems will search the desired infrastructures from its lookup services and return the possible infrastructure's general information and URL. By browsing the infrastructure's XML-based web, clients can check the real time statuses and internal states of the interested infrastructures.

4. Summary

The information revolution has introduced computer and internet into every corner of our society and today we are relying more and more on the computer-controlled systems. However, computer-driven systems are vulnerable to intrusion and destruction. The recent DDoS attacks against e-commerce companies have brought with them the big concern in how to cope with cybercrime and cyberterrorism. Later, by attacking some critical information infrastructure systems, terrorists can easily cause a huge catastrophe to this nation. So how can we protect our national critical infrastructures from the more active and dangerous cyberterrorism? In this paper, we proposed six stages for the information infrastructure protection: intelligence gathering, analysis, interdiction, detection, response and recovery, and our vision for how these stages can be integrated. Meanwhile, some ingredients of these stages are also discussed. To realize the proposed vision, the infrastructure web system is designed as a platform for decentralized monitoring and managing critical national infrastructures.

Currently we are still investigating the possible technologies for the various stages and discussing how to integrate, coordinate, and manage these stages. Meanwhile, the infrastructure web system and sensor web system are under development.

References

[1] http://www.sans.org/ddos_roadmap.htm
[2] http://www.cert.org
[3] http://www.darpa.mil/iso/ia/
[4] http://informant.dartmouth.edu
[5] Lipsey, Richard G. and Courant, Paul N., 1996, Economics 11th Edition. Social and Environmental Regulation. New York: HarperCollins Publishers Inc.
[6] Marcus, Alfred A., 1994, Environmental Encyclopedia. Cost-Benefit Analysis. Detroit: Gale Research International Limited.
[7] Edwards, W.K.,1999. Core Jini. Prentice Hall.
[8] Harold, E.R., 1999. XML Bible. IDG Books Worldwide.
[9] Bertsekas, D.P.& Tsitsiklis,J.N., 1996, Neuro-Dynamic Programming, Athena Scientific, MA.
[10] Weber, J.L., 1998, Using Java 1.2, Que Publishing.
[11] Michael G. Corr and C. Okino. A Study of Distributed Smart Sensor Networks, Dartmouth College, Thayer School of Engineering, Technical Report Preprint, March 2000.

[1] This research has been supported by the National Institute of Justice (Office of Science and Technology), the National Science Foundation, Defense Advanced Research Projects Agency and the Air Force Office of Scientific Research. All opinions expressed here are solely those of the authors.

[2] Authors' email addresses: Cybenko: gvc@dartmouth.edu; Jiang: gfj@dartmouth.edu

Mobile Code: Emerging Cyberthreats and Protection Techniques

Jian Zhao, Ph.D.

Abstract

The response to the future biological threats will be to create a national emergent response network that will remotely operate robots and other countermeasure devices. A major concern in any effort to respond to a biological terrorist attack is protecting the emergent response network that will remotely operate these robots and devices. Protection is also necessary for financial, communications, and utility computer networks against attacks intended to cripple the U.S. economy. Terrorist groups may want to bypass our strength our military to weaken our economy through the private sector. Mobile code, which is originated from a remote, possibly untrusted system, but executed on the local or another remote system, has become part of the modern information infrastructure and is also a crucial component in the future intelligent and autonomous robots. Developing newer and better authentication and encryption techniques are vital for protecting the emergent response network and these robots from cyberattacks.

Key words: Cyberattack, Mobile Code Security, Obfuscation, Digital Watermarking, Encryption, Virus.

1. Roles of Mobile Code

Robots and other remotely controlled devices play a critical role both during the attack and in the clean-up phase after the direct bio-attacks. In both cases, they face a hazardous and hostile environment. While the survivability of the equipment in physical and chemical durability is critical, the countermeasures for these devices against cyber-attack are even more critical because they are networked and remotely controlled. For example, our robots may turn malicious if the attackers intrude into the response network, take over their controls, and modify their behavior.

As more and more of the devices attached to networks have become programmable, *mobile code* has become more and more important. Mobile code is code that is downloaded to a device attached to a network in the course of an interaction between the device's user and the network (or another device attached to the network) and is then executed as part of the interaction. Mobile code is ubiquitous in the Internet. Many Web pages include mobile code written in the Java™ or ActiveX programming languages. Mobile code is also used to implement features in devices such as cellular telephones. When a user accesses one of these features on a cellular telephone, mobile code for the feature is downloaded to the cellular telephone and then used in the interactions that involve the feature. Jini“ from Sun Microsystems, Inc. is a promising technology based on Java, providing simple mechanisms that enable various devices to plug together to form a community. Each device provides services that other devices in the community may use. These devices provide their own interfaces, which ensures reliability and compatibility.

When mobile code becomes an autonomous program and travels from host to host on a network, it evolves into mobile agents. Compared to mobile code, mobile agents typically move from host to host to accomplish specified missions autonomously and collaboratively.

2. Threats of Mobile Code

While mobile code is useful, it can be dangerous both to the device that receives the code and to the system that provides the code for downloading. The danger to the receiving system is that the code may not be what it appears to be. It may have been modified to include a virus or an Internet worm that can damage the receiving system, or it may have been modified to return different or additional data or even to return the data to a different location. This compromises the security of the sending system because the code being executed is not the code that was sent, and the resulting data returned by the receiving system may be altered or infected. To thwart such attacks, the receiving system must be able to identify code that *appears* to come from the legitimate system but has actually been modified to include a virus or to otherwise change the code's behavior. Likewise, the sending system must ensure that the data received from the execution of mobile code on the receiving system is coming from an execution of the original, unaltered code that the sending system *provided to* the receiving system.

3. Authentication of Mobile Code

The inherent dangers of mobile code can be reduced by authenticating the code. One way of doing this is authentication with a digital certificate; the mobile code is digitally signed with a digital certificate issued by a trusted party. However, authenticated mobile code is not necessarily "trusted and safe". There are three difficulties with this kind of authentication:

- It only guarantees that the mobile code has not been modified in its trip through the network; it does not guarantee that the code was not modified *prior* to being sent.
- It cannot guarantee that the receiving system is actually executing the code that it received from the sending system.
- It does not provide authentication on the signed mobile code if the sending system or the key of the sender is compromised.

Furthermore, it is expensive to deploy and maintain digital certificates based on PKI (Public Key Infrastructure). At present, PKI is a common tool for business uses only, and it is unlikely that it will be widely utilized by end-users in te near future.

Additional innovative authentication functions are needed for mobile code. One approach is to apply digital fingerprinting to authenticate mobile code. Analogous to biometric authentication for access control, a digital fingerprint of mobile code is a unique authentication code that is an integral and intrinsic part of the thing being authenticated. It is placed into the mobile code during its development by using digital watermarking techniques.

The difficulty with applying standard digital watermarking techniques to mobile code is that mobile code is executable code; that is, everything in it is functional. There is thus no “noise” to hide the watermark in and adding “noise” changes the behavior of the program. Techniques have nevertheless been proposed for using watermarks to authenticate executable code. These techniques have fallen into two broad classes: *static* watermarking and *dynamic* watermarking. While the static watermark is embedded statically in the program’s object code and can be perceived from the text of the code, the dynamic watermark is embedded dynamically in the execution states of a program and can be perceived from properties of the execution of the code. For example, stack is one of the most important execution states of any mobile code. Figure 1 shows a unique stack trace of a code execution.

Figure 1. Visual presentation of stack monitor extracted from traces of a Java application

[Figure: SEE ATTACHED FILE]

One way to apply watermarking to authentication is to make such static/dynamic watermarks very “fragile” or “sensitive” to any modification of the watermarked code. In other words, any modification will make the watermark undetectable or changed so that the integrity of the code can be verified. Another more powerful approach is to embed a secure hash value or digital signature of the mobile code into the code as a watermark. Such a hash value or digital signature is a unique ID or fingerprint of the mobile code. Any modification on the mobile code results in a different ID. Moreover, it might be more desirable to use the semantic information extracted from the mobile code to produce such a unique ID. Thus, only changes that modify the semantic information of the mobile code will make the authentication fail.

4. Obfuscation of Mobile Code

From the perspective of the owner of the intellectual property rights in a piece of mobile code, the very mobility and portability of the code is a problem. In order to be useful across platforms, the code must be downloaded to the user and executed on the various platforms. Using tools such as decompilers, disassemblers or debuggers, the skilled user can learn a great deal about the mobile code and can use what he or she learns to produce his or her own version of it. Moreover, it allows hackers to easily explore the bugs and introduce virus into legitimate mobile code.

A technique that has been widely used to make the study of programs generally, and mobile programs in particular, more difficult is *obfuscation*. To obfuscate a program, one rewrites it in a form that does not substantially affect the manner in which the program executes, but does make the program more difficult to study. For example, most of the entities in a program have names chosen by the programmer. Programmers generally choose the names with an eye to making the program more understandable for human readers. For the systems that are used to generate executable code from the program or to execute the code, though, it makes no difference whether a name is understandable. These systems require only that the name be used according to the rules of the relevant programming language. Thus, one simple way of obfuscating a program is to replace all of the names in the program with names that are legal in the programming language but as meaningless as possible to a human being reading the program.

```
import java.util.Date;

public class Person {
  private String name;
  private Date dob; // data of birth
  public Person(String n, Date d)
  {
name = n;
dob = d;
  }
  public void changeName(String newName)
  {
        name = newName;
  }
}
```

```
import java.util.Date;
import java.util.Vector;

public class Person {
  private Vector v = new Vector();
  public Person(String n, Date d)
  {
        v.addElement(n);
        v.addElement(d);
  }
  public void changeName(String newName)
  {
        String s=(String)v.elementAt(0);
        s = newName;
        v.setElementAt(s, 0);
  }
}
```

Figure 2. The original code and obfuscated code (data obfuscation)

There exist many advanced obfuscation techniques. For example, data obfuscation changes the storage modes, encoding methods, aggregation, and/or ordering of data structures. Control obfuscation may hide the real control flow behind irrelevant or never executed statements, or change the reducible code to non-reducible. Figure 2 shows the original Java code and the obfuscated Java code in which two data fields are hidden based on data obfuscation. Java from Sun Microsystems, Inc. is one of the most widely used programming languages for mobile code. In the following, we will take Java as an example of mobile code language.

Applying the name obfuscation again to the obfuscated code, we can obtain the following version as shown in Figure 3.

```
import java.util.Date;
import java.util.Vector;

public class P {
  private Vector v = new Vector();
  public P(String n, Date d)
  {
        v.addElement(n);
        v.addElement(d);
  }
  public void c(String n)
  {
        String s=(String)v.elementAt(0);
        s = n;
        v.setElementAt(s, 0);
  }
}
```

Figure 3. Obfuscated code (data and name obfuscation)

5. Direct Execution of Encrypted Mobile Code

One of the most powerful methods is to obfuscate not only the application but also the mobile code in system-provided libraries such as Java SDK (Software Development Kit) to achieve *complete obfuscation*. Obfuscation of such externally defined constructs (classes, methods, statements, etc.) can be done by relating the externally defined construct to an obfuscation for the construct that is used within the executable code. The relationship is defined in a portion of the executable code, and at a minimum, the externally defined construct is encrypted in the portion. When the executable code is executed, a key and cryptographic apparatus are used to relate the encrypted construct to its original definitions. This can be done by using a decryption key to decrypt the encrypted construct and then relating the decrypted construct to the external definition. It can also be done by using an encryption key to encrypt the original externally defined construct and applying that second encrypted construct to the first encrypted construct in the program, thereby relating the external definition to the obfuscation.

```
public class P {
        private V v = new V();
        public P(S n, D d) // constructor
        {
                v.a(n);
                v.a(d);
        }
        public void c(S n)
        {
                S s = (S)v.b(0);
                s = n;
                v.c(s, 0);
        }
}
```

Figure 4. Complete obfuscation

As shown in Figure 3, the Java system class names String, Date, and Vector are not obfuscated. In Figure 4, the system names (key words) String, Date, and Vector are replaced with S, D, and V, and the three system methods Vector: addElement, elementAt and setElementAt are replaced with a, b, and c.

As an extreme case of the complete obfuscation, the mobile code can be cryptographically encrypted. In this case, every component of the mobile code, including operation codes and definitions, whether internal to the code or external to the code, is encrypted. The technique of encrypting the original constructs and then matching them with the encrypted code can even be used to execute encrypted mobile code without decrypting it. When this technique is used with completely encrypted executable code, the encryption may make traditional obfuscation unnecessary.

6. Conclusions

Mobile code has become part of the modern information infrastructure due to its mobility and portability. At the same time, it has also become the first choice of attack tools for hackers. The recent most widely spread viruses, such as LoveBug, are examples how hackers can take advantage of mobile code features. These examples also show the lack of security for mobile code. Even worse, much more sophisticated and harmful malicious code will keep appearing in the future, based on the security weakness of mobile code.

Mobile code is also a crucial component in the future intelligent and autonomous robots that are designed for both active and passive defense against biological attacks. Robots can be dispatched for rapidly identifying biological agents with instant analysis and communications capabilities. Equipped with self-configuration and mobile code, robots may further intercept the delivery system and destroy the enemy biological facilities. For the passive defense, aimed at minimizing casualties after the attack, various robots can be designed for on-site treatment, telemedicine, and decontamination. However, to ensure that the robots' missions are completed as intended, methods for securing the mobile code that directs them must be protected from malicious attacks. Developing newer and better authentication and encryption techniques is vital for protecting these robots from cyberattacks that may compromise their missions.

Digital Medical Information and Relevant Security Issues

Bill Reinsch

The technological revolution of the information age is fundamentally affecting the economy of the United States. Industries are being streamlined and wasteful business practices eliminated in the quest for increased productivity. The medical industry, and its strife with inefficiencies, is a prime candidate for reform. It is the largest vertical market in the United States with costs of about a trillion dollars per year. Annually there are 4 million babies delivered, 762 million physician visits, and 539 million hospital days[1]. For the most part, it is marvelously effective, and even generates a trade surplus for the country. However, healthcare consumers still suffer hour-long waits, uncommunicative providers, confusing and fragmented sources of care, inconvenient locations, and skyrocketing costs.

New technologies, and in particular the Internet, have the potential to automate workflows and bring together the many different industry players, including physicians, patients, labs, insurance companies, and pharmacies. There exists, realistically, the promise of a system that can deliver customer-focused, convenient, courteous, reasonably priced, informative, and easy-to-use products and services.

Embracing new technology, however, brings with it certain risks. This paper addresses the inherent dangers of a digital healthcare system with an emphasis on computer security and data integrity. For the purposes of this study, I will not distinguish between computer systems (boxes with processors and memory) and information technology systems (closely coupled networks of computer systems). Technology has progressed to the point where the lines between software applications and operating systems, computers and networks, servers and browsers are blurred and such dichotomy would be futile.

Security

Security, generally speaking, is about the protection of assets. While a comprehensive information security strategy would have to include risk analyses, that is beyond the scope of this paper and I will assume that relevant data includes all mission critical information. A classifica

---

[1] Regina Herzlinger, Market-Driven Healthcare (Massachusetts: Perseus Books, 1997) xxiv.

tion of protective measures, then, would have to include the following:

- **Prevention**: measures that prevent your assets from being damaged.
- **Detection**: measures that allow you to detect when an asset has been damaged, how it has been damaged, and who has caused the damage.
- **Reaction**: measures that allow you to recover your assets, or to recover from damage to your assets.

Regardless of whether they are online or how sophisticated their business practices may be, medical professionals and those in the industry still have to deal with "real-world" issues of security and the protection of confidential information. Of most concern would be the loss or inadvertent disclosure of any files and data that would infringe upon healthcare consumers privacy: medical records describing conditions, records listing medications, lab results, and insurance information.

Computer Security

Computer security issues, in addition to the above, emphasize data integrity. The three most common ways in which information can be compromised include the following:

- **Confidentiality**: prevention of unauthorized disclosure of information.
- **Integrity**: prevention of unauthorized modification of information.
- **Availability**: prevention of unauthorized withholding of information or resources.

The above definitions are general and, in academic circles, precise definitions are still open to debate. Furthermore, it can be argued that the list is incomplete, and that authenticity (legitimacy of information) and accountability (actions affecting security can be traced) should be included as well. As a broad statement, one could say that computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

Over time, as the number of users in the healthcare industry has increased, the requirements of computer s have evolved accordingly. Thus, a fundamental dilemma for the architects of computer security systems has arisen   security-unaware users have specific requirements, but usually no security expertise. This is an important consideration when designing a security system.

Additionally, there are other operational cost considerations as well. Security mechanisms require additional computer resources. There is also the cost from the inherent trade-off between ease-of-use and engineering. Security potentially interferes with the working patterns users are accustomed to. Productivity is decreased by clumsy or inappropriate security design and restrictions. Effort must also be spent on managing security. While security is a cost that must be justified, it is a generally considered a worthwhile expense in the medical industry.

Principles of Computer Security

There are certain principles of computer security fundamental to the design of a reliable system. These design parameters focus on two areas illustrated by the diagram below. The first dimension is security policy, represented by the horizontal axis, and the second is the layer of the computer system in which a protection mechanism is implemented, represented by the vertical axis[2].

There are five important design decisions to be made when implementing a security system. The first deals with integrity and compliance with a pre-determined set of rules. These rules can cover the format and content of data items, operations that may be performed on a data item, and users who are allowed to access a data item. Thus, the first design decision, at the most basic level, is the following:

- **1st design decision**: Should the protection mechanism in a computer system focus on data, operations, or users?

---

2 Dieter Golmann, Computer Security (England: John Wiley & Sons Ltd, 1999) 12.

The following figure represents a simple layered model of an IT system[3]:

[Figure: SEE ATTACHED FILE]

The layers are broken into five main sections. Users run application programs that have been tailored to meet specific needs. Application programs, in turn, may make use of the services provided by a general purpose software package like a database management system. Running underneath of software packages is the operating system(OS), which performs file and memory management and controls access to resources like printers and I/O devices. A kernel is a piece of the OS that mediates every access to the processor and to memory. Hardware includes the physical devices such as processors and memory that manipulate data held in the computer system. Security controls can be placed in any of these layers, leading us to the next design decision:

- **2nd design decision**: In which layer of an IT system should a security mechanism be placed?

Security mechanisms will often be placed at every layer of the system. Mechanisms at the top layer tend to emphasize the user while those closer to the bottom layer are more computer-oriented.

The next design decision deals with complexity:

- **3rd design decision**: Is the preference for simplicity and assurance or a feature-rich system?

When designing a system, there exists a correlation between the complexity of a system and the level of security. Simple, generic mechanisms won t match specific protection requirements, while a feature-rich security environment will require the users to be experts. The more assurance one wants, the simpler the system will have to be. Given the end users in a medical setting and their relative lack of IT knowledge, this is an important consideration.

---

3 Dieter Golmann, Computer Security (England: John Wiley & Sons Ltd, 1999) 13.

Defining and enforcing security controls is another thing to consider:

- **4th design decision**: Should a central entity, or individual components of a system, be charged with defining and enforcing security?

If there is one central entity or individual charged with managing security, it is easier to achieve uniformity across the entire system. However, a central entity may ultimately end up affecting performance. A distributed solution may be more efficient, although more effort will be needed to ensure that the different components reflect a consistent policy.

The final design decision also deals with the layers of an IT system:

- **5th design decision**: How can one prevent an attacker from gaining access to a layer below the protection mechanism?

Every security system has a defined boundary or security perimeter. This perimeter divides the integral components of a security solution. The parts on the outside can malfunction without compromising the security mechanism, while those that are critical to the system and can be used to disable the protection mechanism, lie on the inside. For example, if a hacker gains system privileges in the operating system, he will usually be able to modify programs or files containing control data for security mechanisms in the services and applications layers.

Identification and Authentication

Identification and authentication are two critical components of any security mechanism that requires user access, and thus warrant some discussion. The user needs to be authenticated because he or she is a parameter in access control decisions. The user s identity is also vital information when creating an audit trail of security relevant events.

When a user sits down at a computer to access a closed, secure system, he or she is usually asked to enter a user name followed by a password. The first step in the process is identification, or announcing who you are, and the second is authentication, or the process of verifying a claimed identity. Once the user name and password are entered, the computer will compare the input against the entries stored in a password file. A valid user name and corresponding password will lead to a successful login.

Currently, most computer systems use identification and authentication (user name and password) as a first line of security defense. It is a mechanism widely accepted and fairly easy to implement. However, obtaining an unauthorized password is also one of the most common ways of hacking into a computer system. There are three ways one could go about doing this:

- password guessing;
- password spoofing;
- compromising the password file.

With password guessing, attackers will follow two guessing strategies. The first is a brute force exhaustive search where the attacker will try all possible combinations of valid characters and symbols up to a certain length. The second method is an intelligent search where the attacker will try passwords associated with a user, such as a name, names of friends, phone numbers, or just passwords that are popular. The attacker may try a dictionary attack, which is an attack using all the passwords from an online dictionary.

From a user s standpoint, a number of preventative measures can be taken.

- **Set a password**: this may seem obvious, but if users forget to set a password for their account, the attacker is spared the trouble of guessing the password entirely.

- **Change default passwords**: when a user account is created by the system, the user is often-times assigned a default password. The assigned passwords are usually easier to guess because they may be linked to the user s identity, such as a social security number.
- **Password length**: exhaustive searches are less effective the longer the password, so a minimal password length should be implemented.
- **Password format**: mixing upper and lower case characters along with numerical and non-alphabetical symbols makes it more difficult to guess a password.
- **Avoid obvious passwords**: using popular passwords found in online dictionaries only makes it easier for an attacker to gain entry.

Additionally, there are some measures that can be taken on the security system side.

- **Password checkers**: a system manager can use tools that imitate an attack and deter many weak passwords.
- **Password generation**: some systems generate a difficult to guess password for the user.
- **Password ageing**: by setting an expiration date, users are forced to create new pass words. This is effective provided users don t always rely on a favorite, trusted password.
- **Limit login attempts**: the system can monitor unsuccessful login attempts and log the user out completely or for a certain period of time to prevent or discourage further login attempts.
- **Inform user**: after login, the system can display the time of the last login and the number of failed login attempts to warn the user about attempted attacks.

There is an additional problem with the identification and authorization method, and that is that it is a unilateral procedure. In other words, there is no guarantee that the only party receiving the entered information is the computer system. This leads to the second way in which a password can be compromised and is referred to as a spoofing attack. In this kind of attack, a program is run presenting a fake login screen on a terminal or workstation. An unsuspecting user comes to the terminal and unsuccessfully tries to login. The false screen queries the user for his name and password, which are then recorded and stored by the attacker. The spoofing program terminates once it has the information, usually by presenting a fake error message. Control is returned to the operating system which now prompts the user for a genuine login and the user is successful the second time around, unaware that the password has even been compromised. The best precautionary methods to take against spoofing attacks are to:

- **Display the number of failed logins**: if there has been a failed login attempt since the last session, but it was recorded, the user could suspect a spoof attack.
- **Trusted path**: ensure that the user only communicates with the OS and not a spoofing program. This can be done by enacting a secure attention sequence such as CTRL+ALT+DEL+ for the Windows NT operating system.

- **Mutual authentication**: this just means that the system would somehow have to authenticate itself to the user.

The third way in which password security can be compromised is the actual modification of the password file on the system. To verify a user s identity, the system compares the user s login to his stored password in the file. A security system should take the extra precaution of implementing cryptographic protection of the file, strict access control enforced by the OS, or a combination of the two.

One last method of fortifying the identification and authentication password procedure is by having multiple logins to different information. Most computer security systems only require a single password. Once it is entered, the user has access to all the information available in a given system. However, forcing a user to remember five different passwords substantially decreases the usability and efficiency of a system. Rather than using passwords, though, a system might authenticate a user based on something the user knows, something the user holds, what the user does, or where the user is. In certain professions within the financial industry in which the user is accessing sensitive information, in addition to a user login and password, the user is given a smart ID card. The card is the size of a credit card and has an LCD display that cycles a string of numbers. Each card is unique to a particular user and the numbers cycling in the card s display are synchronized with the numbers in the system, thus allowing entry given a correct login. This provides an additional layer of security. However, it is unlikely the medical industry has the kind of resources necessary to implement such a strategy, nor would it be necessary. Access to one s medical records is hardly on par with the ability to buy and sell millions of dollars worth of securities without authorization.

How Things Go Wrong

Fortunately, there has have not been well-publicized incidents of security gaffes when it comes to digital medical records. Most of the time when something goes wrong the media picks up on it, but in this case the news has been conspicuously absent. When things do go wrong, however, they can usually be traced back to three things:

- **Change;**
- **Complacency;**
- **Convenience.**

While implementing a complex security system is challenging, more often than not the bugs in the OS or software that allow for penetration are simple programming errors. In many cases attackers exploit well-known security weaknesses in an automated and efficient manner in ways that don t require ingenuity or superior technical knowledge. Following are more detailed explainations of the major sources of security problems:

- **Change in environment**

  Change is arguably most responsible for security flaws. A system might be perfectly ade quate until modifications are made, even if they are as minor as software or operating sys tem updates. The interaction of software, especially what is not apparently visible or what is undocumented, creates a problem for security administrators even if they are aware of the changes implemented.

- **Bound and syntax checking**

  Commands that do not check the size or syntax of their arguments are a frequent source of security problems. By overrunning an input buffer, an attacker with detailed system knowledge can overwrite memory locations holding security-relevant data.

- **Convenient but dangerous design features**

  The more features available the more likely a system is buggy. Features range from ease of installation, ease of use, and backward compatibility with legacy systems.

- **Escapes from controlled invocation**

  Controlled invocation is a process by which a system only performs a predefined set of operations in supervisor mode before returning control back to the user in user mode. This would happen if the user, for instance, wanted to write to a memory location. An error in such a procedure would allow the attacker to ignore the return code and write to the authorization file, which should have been closed by the system.

- **Bypass at a lower layer**

  Logical access control validates users and processes to logical system objects. If an attacker can insert code below logical access control, the security mechanism can be bypassed.

- **Flaws in protocol implementations**

  Programming errors in implementation, while undetected by the programmer, are a source of security holes.

Computer Viruses

Computer viruses have been well documented in the popular press because the direct and visible effects are readily observable. While certainly a security threat, some experts will say that they receive too much attention and are only part of a much wider problem. Viruses first became more of a threat in the business community when PCs gained widespread use in place of main-frames controlled by a central IT department. A computer virus can be defined as a piece of self-replicating code attached to some other piece of code with a payload, ranging from the non-existent or harmless (like displaying a message), or the harmful (like deleting and corrupting files). The virus infects a program by inserting itself into the program code. There are a few different types of viruses: a Trojan horse is a program with hidden side-effects that are not specified in the program documentation and are not intended by the user executing the program. A transient virus is only active when the program it has infected is running. A resident virus establishes itself in memory when the program it has infected is running; it can become active even after the program it was attached to has terminated by linking itself into other programs. A logical bomb is a program that is executed only when a specific trigger condition is met. And last, a worm is a replicating but not infecting program. Furthermore, a virus can be classified by its point of exploitation.

- **Bootstrap virus**
  A bootstrap virus enters a system on an infected storage medium such as a floppy disk.
- **Parasitic virus**
  A parasitic virus is attached to an executable program and infects other programs. This kind of virus commonly appends itself to the infected program and inserts s jump to the viral code at the beginning of the program. At the end of the virus there is a jump back to the start of the program.
- **Companion virus**
  A companion virus, in DOS, exploits the default system searchpath by naming itself after another file while changing the extension, for example, from an .exe to a .com so that the virus application is launched unknowingly.
- **Macro virus**
  A macro virus can attach itself to a spreadsheet or data file. These can be particularly damaging because they may bypass integrity protection mechanisms targeting normal exe cutables such as the OS or programs. The virus is written in a high-level language so it is more platform independent. And lastly, text documents are widely exchanged by email, and ideal medium by which a virus can spread.

Commercial virus-protection software is widely available and serves as a more than adequate security measure as long as the virus definitions are updated. Any defensive strategy or software must encompass the processes of prevention, detection, and reaction.

World Wide Web Security

In a nutshell, the Internet and the World Wide Web have changed the nature of distributed computing. While the Web has not created fundamentally new security problems, it has changed the context in which security has to be enforced. The following key observations can be made:

- Programs and data are essentially indistinguishable. Content providers embed executable content (applets) in documents to create interactive web pages that can process user input.
- Computation is moved to the client. Clients now need protection from content

providers.

• Mobile code moves from machine to machine collecting information or searching for computing resources. Clients need protection from mobile code; and mobile code may need protection from the machine it is running on.

• Users must now become system administrators and policy makers.

To access the World Wide Web, a client needs a web browser, a simple program that presents the user with a graphical user interface and includes the necessary protocols to connect to the web. The browser:

• Is the interface for viewing web pages;

• Is a service layer for applications;

• Includes protocols for communication with web servers;

• Manages security relevant information for the client.

The main components of the web security model are the client, the client s browser, and the web server. Browsers essentially become part of the computing platform once they are connected to the Internet.

• The browser handles the client s web traffic. To ensure the smooth transfer of content between client and server, the browser provides information about the user and the user s computing environment to the server. One important consideration is privacy protection because the server is in a position to build up a database about its clients.

• Browsers manage the default settings and preferences for client environments. These include security preferences.

• The browser is entrusted with the client s private keys when performing tasks related to encryption for the client.

• Overall, browsers assume more functions originally designated for the operating sys tem. In the process, browsers have taken on security-relevant tasks such as user authen tication, either to control access to the browser itself or to control access to certain web pages.

In order to fully utilize the power of web technology, users must be willing to accept executable content (applets) from web sites they visit. To ensure security, they must be able to control the actions of applets in a somewhat demanding environment:

• Users won t have a prior relationship or trust with the source of an applet.

• Few users are willing to decide personally on each access request made by an applet because it would be a hindrance.

• The client s OS cannot be expected to offer any protection.

Platform independent applets are written in Java, a versatile language designed by Sun Microsystems. Security considerations were part of the design decisions made:

• The language itself should make it more difficult for programs to create damage.

• The execution environment provides mechanisms for access control.

- The security policies enforced by the execution environment must be set correctly and in place.

As a result applets are run in a secure fashion:

- Applets do not get access to the user s file system.
- Applets cannot obtain information about the user s name, e-mail address, or other personal information.
- Applets may make outward connections only back to the server from which they came.
- Applets cannot reconfigure the system.

Conclusion

Designers of information technology systems for the medical industry must still consider general computer security issues such as those mentioned above. When evaluating the overall structure of a system, important considerations are functionality (the features of a system), effectiveness (are the mechanisms appropriate?), and assurance (thoroughness of the mechanisms).

Thus far, media attention given to the healthcare industry in the information age has been mostly limited to privacy issues. Part of the reason for this is that the industry has been slow to utilize modern technologies — the paperless office is still a pipe dream, albeit a more realistic one. However, as physicians, patients, and other players find themselves more interconnected, they will need to give to give more attention to security issues.

References

Amoroso, E. Fundamentals of Computer Security Technology. New Jersey: Prentice-Hall International, 1994.

Cheswick, W.R., and S.M. Bellovin. Internet Security. Massachusetts: Addison Wesley, 1996.

Curry, D.A. Unix System Security. Massachusetts: Addison-Wesley, 1992.

Ford, W. Computer Communications Security. New Jersey: Prentice Hall, 1994.

Gasser, M. Building a Secure Computer System. New York: Van Nostrand Reinhold, 1988.

Gollman, D. Computer Security. Chichester: John Wiley & Sons, 1999.

McGraw, G., and E.W. Felton. Java Security. New York: John Wiley & Sons, 1997.

Pfleeger, C.P. Security in Computing. New Jersey: Prentice-Hall, 1997.

Russel, D., and G.T. Gangemi, Sr. Computer Security Basics. California: O Reilly and Associates, 1991.

Smith, M. Commonsense Computer Security. London: McGraw Hill, 1993.

Sutton, S.A. Windows NT Security Guide. Massachusetts: Addison Wesley Developers Press, 1996.

Emerging Technologies for Response to Weapons of Mass Destruction

Joseph Rosen, MD

The major focus of this report is to identify emerging technologies that can be used to respond to terrorist threats. We are particularly interested in emerging technology that can be used for education, training, simulation, and predicting the outcomes of our operational plans. From our initial meeting in July our goal was to produce a number of recommendations. We further refined these recommendations in a September meeting. Following that, in a series of meetings in October and November, we further refined these recommendations through meetings with operators, policy makers, and technologists.

We took a paper by David Franz and expanded it with input from a small ad hoc group in our September meeting. Included in our list of recommendation are: (1) Technology base: research and development; (2) Intelligence and surveillance; (3) Forensics; (4) Proactive deterrence; (5) Medical countermeasures; (6) Physical countermeasures; (7) Public Health infrastructure; (8) Interagency collaboration; (9) Education; (10) Complementary programs; (11) International cooperation; and (12) New technologies. Our white paper in this section goes into each of these areas in more depth. White papers in our edited volume and references that we cite also go into each of these areas in more depth.

However, our overarching recommendation is to use virtual reality and advanced simulators to create a comprehensive system for counterterrorism. This would be enabled through the creation of a large-scale virtual reality simulation environment as a national center that would integrate our policies, operational plans, emerging threats, and responses within a single framework. The center would exist in cyberspace and have multiple sites throughout the country that could interact on a frequent and on-going basis.

It would take advantage of emerging technology over the past decade that has allowed both the civilian and defense communities to simulate and train for difficult and unusual tasks. The simulation center concept is built upon emerging technologies that have been developed over the past ten years in both the civilian and defense communities (see NAS report on virtual reality 1995, and Nasal Studies Board report 1997 that covered the timeline between 2000 and 2035 and the DMSO web site).

Information technologies combined with virtual reality can be used to create an environment that will allow us to test out our concepts in counterterrorism. In particular, it will allow us to connect our policy and strategy to our operational plans, providing rapid proof by concept analyses of emerging technologies, and demonstrating the role they can play in our antiterrorist efforts. Emerging technologies for responses can be introduced into our simulated worlds to test if they can affect significant improvements in our operation plans.

Simulators have been designed and implemented for small engagements and large-scale event training. Simulators that have been developed to train small engagements of individuals in difficult tasks have been used for flight simulation, urban warfare, and medical response teams. The medical training of first responders in a bioweapons attack could be crucial to the success of providing vaccines and antibiotic treatments when indicated.

Large-scale simulators have been used to model entire battles involving large numbers on manned vehicles for the Gulf War (73 easting/DMSO), by the army, air force, marines, and navy. Their time scales can be real time, or can be altered to allow high levels interactions. A large-scale simulator has not yet been used for simulating mass casualty events for the Department of Justice.

In these simulators, virtual humans are used to simulate casualties, terrorists, and first responders. Their simulators can act according to some predetermined script, or they can be operated or controlled by people assigned to manipulate them for the training session. Some of the virtual humans have been developed to accurately simulate the effect of conventional weapons injuries. For example, they could predict the effect of a gun-shot wound to the leg — the ability of the wounded individual to survive and walk, and how best to repair or stabilize the injury.

Simulators can be used in the actual performance of the task. A simple example of this is in remote operations or tele-operations. In tele-operations, simulators can first be used to practice a task. They then can be used in the performance of the task. In the first case the environment is completely modeled. In the tele-operated case the model can be super-imposed on the actual physical reality. This is often referred to as augmented reality or datafusion. It is used in neurosurgery and is also used in special military exercises. It allows soldiers or surgeons to seamlessly transfer their training from a practice case to the real case.

When operators, such as first responders, are being assisted by virtual mentors that appear within their environment, it is called tele-presence. The experts are located at a distant remote safe site and can supervise and advise the actions of first responders who have less knowledge. This is used now in both civilian medical applications and in military applications. When the expert controls a robot, it is called tele-robotics and requires significant bandwidth between the remote site and the site where the robot is providing assistance. At the present time, remotely controlled robots are being used by the justice department for the de-fusing of bombs and in special cases of hostage rescue.

These technologies were first developed for applications to the management of hazardous materials using tele-operations. They have more recently been greatly advanced for telesurgery. These new systems have realistic 3D vision, 3D sound, and sensitive force feedback touch and manipulation interfaces. They are being used more and more in surgery in remote operations. These systems can be used for training, performance of surgery and, in special cases, have been adapted to allow the prediction of outcomes. These performance machines can allow the surgeon to predict what the effect of a specific maneuver would have on the outcome of the patient. The earliest of these systems was developed in the 1990s. It is based on a physical model of the organ or structure being operated on and measures the effect of a set of events on the outcome to the human body. They can also be used to predict the effect of ballistic weapons on the human body.

We recommend the use of virtual reality simulators to bring together the three parts of the counterterrorism system the policy makers, the operators, and the technologists. We then propose that multiple scenarios be tested within these simulation environments to determine the strengths and weaknesses of our operational plans. For example, the template system for a response to a bioweapons attack that is proposed by Dr. Hutchinson could be tested extensively in this system to determine how it could be employed and adapted to different cities. We can see what the effects of specific emerging technologies would be on our response to specific emerging threats. For bioweapons and mass medical casualties we present this simulation system in the white paper entitled MEDNET. With respect to an augmented reality system we present this system in the white paper CYBERCARE. We also included a paper describing an extreme information infrastructure (Bobby Hartway), and a a paper describing cybercare robots (Neil Fisher). These are all possible physical and information technologies that could be used to respond to a large scale strategic terrorist attack and could be tested within an advanced simulation environment.

Global Strategy to Prevent Biological Terrorism

Hon. Michael Moodie, Dr. Andrew Schmookler and Dr. Richard Hutchinson

Aims. This project will bring together some of the best minds from around the world, and from a diversity of areas of expertise, to formulate a comprehensive global strategy to help prevent biological terrorism. The impetus for the project derives from the realization that, as Secretary of Defense Cohen has said, A lone terrorist could hold a city s population hostage with the threat of a biological weapon and unravel the very fabric of our culture - our sense of being safe within our borders (Cohen in Lederberg, 1999, p. xii). The international team will be led through a proven deliberative process to focus on three dimensions of the challenge of prevention: 1) how to reduce the *opportunity* for terrorists to strike their desired targets, 2) how to keep the terrorists from achieving the *means* to deploy biological weapons, and 3) how to reduce the *motivation* of potential terrorists to inflict on world cities the pain and destruction that a biological attack would entail. With respect to each of those goals, priority will be given to identifying those measures that are most feasible, most cost-effective, and most promising of significant impact. Thus, the resulting strategy will encompass an integrated vision to prevent biological terrorism and will also identify practical means to achieve that vision.

The project will produce, as its ultimate fruit, a report intended for publication and widespread dissemination with the goal of mobilizing world opinion in those ways that will support efforts to prevent biological terrorism. Further, this report will provide for U.S. officials insights and policy options to assist them in their efforts to prevent biological terrorism.

Background and Significance. Previous analytic study has indicated that it could be possible for cities to respond effectively to biological attacks if they have an integrated, preplanned response capability, if the medical communities agree to change their methods of operation during a biological terrorist incident and to function under centralized direction, and if communities plan for the rapid application of regional, State and Federal assistance during a biological incident (Hutchinson and Mughal, 1998, pp. 13-15). That analysis suggested that cities prepared to respond effectively to biological attacks could potentially reduce suffering and death by approximately 50%.

However, despite any conceivable improvements in response-capability that might be achieved, even the lowered level of death, suffering and economic loss would remain wholly unacceptable to any humane society. For example, an attack on a subway system with anthrax spores might kill 100,000 people, or perhaps even more. Although the continuous medical surveillance and rapid administration of medication might reduce the number of deaths to 50,000 and reduce the economic impact, in terms of lost future earnings, from $100 billion to $50 billion - the moral impact upon our nation of such an attack would be incalculable (future earnings estimates derived from Kaufmann 1997, pp. 83-94).

Thus, while preparations for effective response are clearly needed, they are not sufficient. Prevention of biological terrorism is essential.

The U.S. law enforcement agencies are enhancing their ability to detect, interdict and prosecute biological terrorists. The U.S. Counterproliferation Initiative and other efforts to develop arms control regimes focus on external threats. These initiatives - in addition to improving response preparations - might also be helpful in deterring biological terrorism. But the effectiveness of all such preventive measures is likely to be limited because of the power, the ease of delivery, and the delayed effects of biological weapons.

The problem may be depicted as a relationship between, on the one hand, U.S. direct prevention, the sum of deterrence, detection, interdiction, response and prosecution, and, on the other hand, the motivation, means and opportunity of terrorists. As Figure 1 suggests, how things tip depends on the location of the fulcrum, which might be understood as being located according to the balance of the advantages and disadvantages impinging upon the two contending sides. For example, the fulcrum could be moved to the left, favoring the terrorists, by such factors as the diversity of biological agents and of the forms they might take, and the ability of the terrorist to choose the time and place of his attack. Also threatening to give the advantage to the terrorist from the other side of the fulcrum could be such potentially disadvantageous factors as the cost to the defending society of making response preparations and the diminishing-return limits on what can be practically achieved.

Figure 1. Balance between direct prevention and terrorist intent and capability.

[Figure: SEE ATTACHED FILE]

The limitations of a strictly American approach to direct prevention can be partially reduced by taking a more global approach to the threat of biological terrorism. By matching the global nature of the problem, the global approach can favorably affect both sides of the balance, both reducing the motivation, means and opportunity of the terrorists through indirect approaches, and expanding the effectiveness of direct prevention measures throughout the world. A unique aspect of this project is its dedication to exploring both the immediate and technical task of directly preventing biological attacks and the longer-term more indirect tasks of reducing the potential sources of hostility, resentment and alienation that might motivate such attacks.

Another reason for global efforts is the way that terrorist incidents elsewhere in theworld could impact American society. Consider that a serious biological terrorism attack on London, Paris, or Tokyo would affect the international economy and, in turn, the U.S. economy. Further, it would affect U.S. moral and sense of security. Witness our response to the sarin gas attack in Tokyo that triggered the Nunn-Lugar-Domenici domestic preparedness program.

Additionally, should biological terrorism come to pass on a significant scale, global order would likely be altered. For example, nuclear warfare has made it impossible, in practical terms, for the strong to wage war on the strong, because of what was called, in the cold war, mutual assured destruction. Likewise, biological warfare, which may make even the mightiest nations vulnerable to unacceptable damage from even minor world actors, may make it impossible, through a similar kind of deterrence, for the strong to wage war on the weak. In view of such potential epochal world changes, it is of vital importance that the various possible scenarios involving the future of biological terrorism be considered in advance and, where possible, steps be taken to influence which of those scenarios becomes the reality.

Preliminary Studies. The present project builds upon prior work that 1) developed a methodology for coordinating the insights of a diverse group of people and 2) explored the benefits and limitations of response-preparation programs for coping with biological attacks after the fact.

The methodology by which this project will elicit the knowledge and insights of the people consulted, and will integrate these ideas into a global strategy to prevent biological terrorism was developed by one of the directors of this project and was previously used by him and his colleagues in the conduct of earlier projects of a complex nature, also involving weapons of mass destruction. This methodology was first devised, in support of U.S. negotiators for the chemical weapons convention, to develop a system of verification measures for that treaty. The methodology consists of a way to focus a group of minds directly on the problem of interest and to proceed through a sequence of concept formulation, component testing and system testing in a manner analogous to the scientific method. It is our experience that this rigorous approach is uniquely suited to address in a meaningful way extremely complex problems such as that of how to prevent biological terrorism.

Under the Nunn-Lugar-Domenici Domestic Preparedness Program, the assessment of response options and the development of an integrated city response strategy for acts of biological terrorism produced an understanding of what can and can not be accomplished through response preparations. These findings are important to the present effort because the relative costs and benefits of the preventive measures arrived at through the present study will be compared to those of the earlier-developed biological response strategies in order to identify more clearly which of the various possible approaches to preventing or mitigating biological terrorism are most cost effective. A summary of this work, which also utilized the methodology discussed above, is available on the Web (Hutchinson and Mughal, 1998).

Experimental Design and Methods. The assessment process will be accomplished by focusing an international team on devising a set of preventive measures to reduce terrorists opportunity, means and motivation to conduct biological terrorism. The team will define each preventive measure in sufficient detail to allow for a comparative evaluation of its likely feasibility, effectiveness, and cost to implement and sustain. The preventive measures with higher feasibility and effectiveness in relation to their cost will then be selected for integration into a comprehensive strategy. The resulting global strategy - the ultimate purpose of the effort - will embody a balanced set of cost-effective preventive measures.

A key early step in the process will be the identification and recruitment of an international team of multi-disciplined, knowledgeable personnel to help in the formulation of a strategy to prevent biological terrorism. To assure consideration of a broad array of preventive measures, the international team will be assembled into six working groups corresponding to six dimensions of the biological terrorism problem. These dimensions, as well as illustrative examples of the types of preventive measures that each group will consider, are listed below.

1. BW experts working group.
    - Identify ways to change attitudes overseas so that biological terrorism is taken seriously and information on response planning is more widely shared.

2. Public health working group.
    - Identify ways to integrate biological response preparations in cities around world, to improve\worldwide surveillance, and to foster more rapid epidemiological investigations.

3. Intelligence, law enforcement and information working group.
    - Identify ways to block the access of radical groups or regimes to biological warfare expertise, such as that of former soviet scientists.

4. Arms control and international law working group.
    - Identify ways to reinforce global norm against biological weapons as abhorrent to civilization, and to strengthen international law by making biological terrorism a crime against humanity, including provisions for individual accountability and punishment.

5. Conflict resolution working group.
    - Identify ways to develop and strengthen various approaches to reducing chronic hostilities across social divisions (e.g. along ethnic or religious lines) and to deal more effectively with tyrannical leaders and rogue states.

6. Conflict avoidance working group.
    - Identify ways to avoid or reduce the clash of civilizations, i.e. of the eruption of fundamental antagonisms between major cultural groupings with different world views.

These working groups will be brought together and focused on the problem of preventing biological terrorism through a series of three workshops. Each working group will include five to six experts from around the world. The types of people needed for each working group are shown in Annex 1 along with a tentative indication of their places of origin. The international team members will be recruited on the basis of their possession of knowledge relevant to one or more subject areas corresponding to the working groups, and will be paid as consultants for their time and travel expenses while participating in the assessment. Each person will be expected to make a commitment to participate throughout the assessment process. Participants will be asked to leave their rank and affiliation at the door and to participate in a peer-group setting, on the premise that good ideas can come from any participant at any time, and that openness is requisite for both the expression and hearing of those good ideas.

The three workshops described below are structured to focus the participants minds on the problem of preventing biological terrorism and to provide a logical sequence of events to identify, assess, and integrate *feasible and cost effective* solutions to this complex international problem. To facilitate an international perspective throughout the effort, the three workshops will be held in different parts of the world.

Workshop #1 (North America). The workshop will begin with a plenary session, in which the international team will be oriented to the study approach, schedule, expectations, and ground rules for our process. Then the team will explore a series of scenarios of possible incidents of international biological terrorism to identify, and then to examine those factors that might be conducive to such attacks. The team will then generalize from these examples to generate a plausible range of motivations, means and opportunities that might lead to biological terrorism. The possible consequences of such attacks will also be considered. The purpose of this exercise will be to develop a common understanding among the participants of the various dimensions of the problem of biological terrorism and, by making the problem concrete, to facilitate the group s identifying possible points of intervention for the prevention of such attacks.

The international team will then break into the six working groups and, through brainstorming, begin to develop a list of possible preventive measures lying within the purview of their respective groups. Each working group will then make a preliminary ranking of the various proposed measures according to their likely effectiveness in preventing biological terrorism, leaving aside, momentarily, the question of achievability. Each preventive measure will then be assigned to a working group member to assemble, for the next workshop, background and historical information pertinent to the challenge of implementing that measure.

The international team will then reconvene in a plenary session for each working group to present to all the others their listing and ranking of measures to prevent biological terrorism. This will give the entire team an appreciation of the scope of all preventive measures being considered. The resulting cross-fertilization of ideas might lead to the identification of additional preventive measures by the group working as a whole, and any such measures will be assigned to a working group for further analysis. After each workshop, the core team - comprised of the three program co-directors - will prepare a workshop report for use by the participants and the sponsors.

<u>Homework assignment between Workshops #1 and #2.</u> As indicated above, working group members will collect and prepare a written summary of useful background and historical information for each of the preventive measures under consideration. This effort will support the subsequent identification of specific steps and actions needed to implement the preventive measures. Working group members will perform this work at their home location and communicate results through e-mail to other working-group members. They will be reimbursed as consultants for the

time spent on the homework assignments up to a predetermined maximum number of hours.

Workshop #2 (Africa). Each working group will brainstorm about the specific steps and actions to implement each preventive measure. Through this effort, the working groups will define each preventive measure in sufficient detail to allow for subsequent evaluation. Then, each working group will consider their set of preventive measures as an interrelated system and will adjust their proposals based on the insights gained. Working groups will then begin to evaluate each preventive measure on the basis of:

1. Effectiveness in preventing biological terrorism if implemented,
2. Feasibility of each measure both politically and technically, and
3. Cost to implement and sustain each preventive measure for 10 years.

The preventive measures will be grouped according to the time-frame for their implementation: near-term (1-4 years to implement), mid-term (5-9 years), and long-term (10 or more years). While evaluations for effectiveness and practicality could be completed during the workshop, additional effort between workshops will likely be needed to complete the cost analysis.

Workshop #2 will end with a plenary session where each working group will present its proposed preventive measures and discuss the steps and actions needed to implement those measures. From this, a view of a possible comprehensive system of preventive measures will begin to emerge.

<u>Homework assignment between Workshop #2 & #3.</u> Individual working group members will develop and refine the estimates of the costs for achieving each preventive measure. The evaluations of effectiveness and feasibility will also be refined. Participants will be encouraged to consult with other experts in making these assessments.

Workshop #3 (Asia). In the final workshop, the working groups will review the final evaluations of their preventive measures. Based on these evaluations, each working group will develop a recommended set of preventive measures. Consideration will be given to the formulation of a balanced mix of short-, mid- and long-term measures.

The working groups will then join a plenary session and report their overall assessments and recommendations. The international team will then consider the preventive measures as a whole. Would they work together? Is the total cost reasonable? Is the mix of short, mid and long-term measures appropriate? Could the list of measures be cut to reduce cost without jeopardizing the overall effectiveness of the proposed system?

The international team will then agree on an integrated system of protective measures and identify the overall strengths and weaknesses of the integrated system. In order to facilitate a more comprehensive cost-benefit analysis, the international team will then identify the benefits that the proposed system, if implemented, might confer upon efforts to address other world problems. The team will also work to devise possible ways to test the preventive measure in order to validate the assessment of their feasibility and cost. Finally, an outline of the final report will be presented for discussion and refinement.

Throughout the three workshops and during the periods between workshops, participants will be encouraged to exchange information and ideas among the various working groups. While the plenary sessions will help in the exchange of information, the informal exchange during informal times like coffee breaks and meals will be equally important. The structure of the workshops themselves will also encourage such synergistic cross-fertilization of perspectives and insights. In addition, a Web page will be established to facilitate exchange of information between participants when they are at their home locations.

Following the third workshop, the core team will prepare and, after review by the participants, publish the final report.

Results and Impacts. The assessment will result in a global strategy to prevent biological terrorism by reducing terrorists motivation, means and opportunity to conduct such terrorism. The strategy will represent an international perspective with input from citizens of both developed and developing nations. Further, the strategy will represent the fusion of a diverse array of possible preventive measures into an integrated system that is feasible and cost effective. The specific steps and actions needed to implement each preventive measure will be included in the description of each measure. A plan for pilot testing components of the strategy will be included in the final report in order subsequently to demonstrate the value and the cost of the preventive measures.

The resulting report will be intended for publication and widespread dissemination with the intention of mobilizing world opinion in ways that will help prevent biological terrorism. Further, this report will provide insights and options to assist U.S. policy officials in their efforts to prevent biological terrorism. The core team will conduct an active effort to present the projects recommendations and findings to key audiences inside and outside of government.

References

Cohen, W. S. in *Biological Weapons, Limiting the Threat* (ed Lederberg, J.) xii (MIT Press, Cambridge MA, 1999).

Hutchinson, R.W. & Mughal, M. A. Biological Warfare Improved Response Program, Executive Summary, 1998 Summary Report on BW Response Template and Response Improvements. www.sbccom.apgea.army.mil/ops/dp/fr/dp_bw_irp_executive_summary.pdf (1999).

Kaufmann, A.F., Meltzer, M.I. & Schmid, G.P. The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable? Emerging Infectious Diseases V3,2, 83-94 (Apr-Jun 1997).

Annex 1.
Working group composition and tentative location of participants.

BW experts working group

U.S. biological warfare program expert (U.S.), Detection specialist (Europe)
Former Soviet Union biological warfare program expert (Former Soviet)
Protection specialist (U.S.), Biotechnology scientist (Japan)

Public health working group

City emergency medical technician (Asia), National public health official (France)
Hospital medical doctor (Africa), City public health official (U.S.)
World Health Organization (United Nations)

Intelligence, law enforcement and information working group

City police inspector (New York City), FBI or Scotland Yards officer (U.S. or England)
Former intelligence officer (U.S. or Europe), Journalist (New York City)
International treaty inspector (United Nations foreign national)
Expert on biological warfare knowledge and expertise

Arms control and international law working group

Australia Group expert (Australia), International law expert (Europe, World Court)
3 Arms control experts (India, Brazil, and Europe)

Conflict resolution working group

2 International law experts (Europe, Asia), Cultural expert (South America)
2 Practitioners on conflict resolution (Middle East, Bosnia)

Hostility avoidance working group

Global ideology expert (U.S.), Multi-national corporation official (Europe)
World Bank (Asia), Developing country global planner (South America)
Religious expert (Africa), Cultural Expert (Asia)

Deterring CBRN Terrorism: Developing a Conceptual Framework

Michael J. Powers

Over the past five years, a great deal of resources — financial resources, intellectual capital, time — have been expended in preparing for and developing a national capacity to respond to incidents of chemical, biological, radiological, and nuclear terrorism (CBRN). These efforts have included substantial federal programs designed to bolster state and local public safety and public health capacities to prevent, detect, and respond to CBRN terrorism. Both executive and legislative branch officials have stated that these programs will detect, thwart, and mitigate the effects of CBRN terrorism, but also deter potential terrorists from using these weapons. But, does it make sense for government officials to talk about deterring CBRN terrorists as part of a national counterterrorism strategy? What does it mean to deter potential terrorists? Is the logic of deterrence useful in addressing this threat? Can potential terrorists be deterred? What about potential CBRN terrorists? What are the available instruments useful in implementing a deterrence strategy with the broader national counterterrorism strategy? How could these various instruments deter potential terrorists? This paper provides a conceptual foundation for developing an integrative policy approach to deterring CBRN terrorism. While the success of a deterrence-oriented approach in preventing an individual act of terrorism ultimately depends on the terrorist s unique set of motivations and logic, casting what Graham Pearson describes as the web of deterrence, has the potential to catch a majority of potential CBRN terrorists. Importantly, deterrence in the context of CBRN terrorism does not require a new set of instruments. Most of the necessary instruments currently exist, and if better integrated, policymakers can exploit them within a deterrence-based framework.

Developing this framework requires elucidating and then integrating the component parts of three distinct, but closely related dimensions. The first dimension, the *elements of deterrence*, is the basic conceptual precept of deterrence theory. The second dimension, *opportunities for deterrence*, is the set of decision points within the process of CBRN terrorism — from group formation to utilization of a CBRN weapon — that could be affected by the instruments of deterrence. The final dimension, the *instruments of deterrence*, is the set of tools use to deter terrorists through their effect on the opportunities. Identifying the range of constituent parts of each produces a matrix that can be used to explore the interaction between opportunities, instruments, and conceptual elements. Figure 1 is a graphical representation of this matrix. Systematically identifying the linkages and relationships between the components of each dimension produces a conceptual framework for developing a deterrence-based approach to countering CBRN terrorism.

Elements of Deterrence

Althought the exact details of how a terrorist develops an interest in CBRN weapons, goes about the task of developing CBRN weapon, and then actually utilizes that weapon will differ in each case, the concept and practice of deterrence has not changed much since the conceptual development and subsequent refinement conducted during the early stages of the American-Soviet nuclear standoff. The core conceptual components of deterrence have remained constant, but have been adjusted in response to changes in current threats, like the Cold War nuclear confrontation, or in new situations to address new types of threats, like the challenge of chemical and biological proliferation. It is important to note that each of the following elements must be present within an effective deterrence strategy. Each conceptual element forms an indispensable part of the concept and practice of deterrence.

Action to Be Deterred

In the CBRN terrorism context, the ultimate action to be deterred is the use of a CBRN weapon by a terrorist. Yet, as the CBRN process model demonstrates, a number of intermediate steps must take place - acquisition of resources necessary to obtain equipment, materials, and expertise, weapon development and production, testing and evaluation, and operational preparations for weapon employment. Each of these intermediate steps also provides an action to deterred. Because of the interrelation of these steps, deterring the terrorist from undertaking any of these steps will prevent the terrorist from successfully acquiring and using CBRN weapons. In this context, the objective of a deterrence strategy should not only be deterring *use* of the weapon, but should also focus on attempting to deter the terrorist from undertaking the intermediate steps.

Target of Deterrence

Any deterrence strategy involves persuading an individual or group from undertaking an unwanted action. At its core, deterrence rests on the ability to influence the decision making process of the individuals undertaking the unwanted action before that action is taken. That individual or set of individuals are the targets of deterrence. For a lone actor, that individual is the sole target. Deterring a group requires an ability to influence the key decision-makers within that group. During the Cold War, the United States and the Soviet Union focused their deterrence efforts on influencing the leadership of the other country. For many (especially contemporary) terrorist groups, a formal leadership structure may be hard to define. Even within rigidly hierarchical groups like states, decision-making does not always rest with the formal leadership — other members of the group are responsible for executing the mandates of the leadership. Because CBRN terrorism is not a single act but a series of actions undertaken by particular individuals, each of whom provides opportunities for deterrence, almost all members of a terrorist organization are potential targets of deterrence. Perhaps the best example of this is the failure of an Aum Shinrikyo cult member to puncture his sarin-filled pouch during the cult s infamous 1995 attack. According to various studies conducted after the attack, he failed to carry out his assignment because he feared arrest and prosecution.

Deterrence requires not only identification of the target of deterrence, but also an understanding of the target. Because it rests on affecting decisions made by the target, deterrence also requires an understanding of how the target, in this case the CBRN terrorist, makes decisions. While most models of deterrence suggest decision-making is a mechanistic process of cost/benefit analysis, in reality, decision-making is a highly complex, psychological process. For both individual terrorists and terrorist groups, decisions are based on a process combining a pure rationality that weighs expected costs with benefits, and degrees of risk associated with taking a certain action, and other non-rational, psychological and social factors, including hatred, fear, obsessions and compulsions, and other factors.

The more that is known about the CBRN terrorist s motivations and values, the better costs and benefits can be manipulated for the purpose of deterring the unwanted action. Thoroughly understanding the group s motivations and values provides the baseline for assessments of the government s ability to manipulate costs, benefits, and risks involved with development and use of a CBRN weapon.

Cost/Benefit Manipulation

The practice of deterrence focuses on exploiting the ability to manipulate the costs and benefits associated with the action being deterred to influence the target s decision to undertake that action. In theory, a reduction of benefits the actor gains, or an increase in incurred costs, will dissuade the actor. Because the incursion of costs, and receipt of benefits occurs *after* undertaking the unwanted act, deterrence requires the target to recognize the deterrer s capability and willingness to manipulate costs and benefits *before* deciding to act. To successfully deter the actors, the unwanted action, the target of deterrence, and in this case the terrorist, must be confident at the point of decision of the deterring party s ability and willingness to manipulate costs and benefits. The key to deterrence is shaping the actor s perception of the costs, benefits, and risks associated with acting *before* he acts.

Cost may be measured by the terrorist in a number of ways, including risk of punishment, wasted financial resources, loss of time, diminished international standing, loss of political support, etc. In this regard, perhaps the strongest cost that can be fostered through deterrence is a personal impact on the freedom of the terrorist, including imprisonment. Increasing the costs incurred by the terrorist after an incident fosters the perception that the risks associated with the undesired action are above acceptable levels. In addition to increasing costs incurred after an incident, steps taken to complicate the process of CBRN weapon acquisition can serve to convince potential terrorists that CBRN weapons are either too difficult to acquire or too expensive.

Equally important to dissuading the potential terrorists from acquiring and using CBRN weapons are demonstrations of effective consequence management and mitigation capabilities.

These capabilities serve to reduce or remove projected benefits from the use of such weapons by minimizing their immediate impact. During the Cold War, all but moderately effective defenses against bombers and ballistic missiles were deemed to be very technically challenging and too expensive to develop and deploy. Because of their enormous destructive power, American government officials abandoned civil defense efforts with the advent of thermonuclear weapons. Because the effects of chemical, biological, and radiological weapons are less immediate, defensive measures can be taken to reduce the effects of these weapons on their victims before the victims are seriously injured. Deterring CBRN terrorism requires convincing the potential CBRN terrorist that potential benefits are minimal or nonexistent.

Communication

Communication with the target plays a pivotal role within a deterrence strategy. Because the key to deterrence is to influence the target s decision-making process by ensuring their awareness of probable costs and benefits, it may be the single most important element of deterrence. This is done by informing the target that the response to acting will impose costs, remove benefits, or increase risks. Effective communication is the mechanism through which the deterrer can provide the actor with this information.

Communication may occur either directly or indirectly. If the target is known, communication can be either direct or indirect. Direct communication can take various forms - phone calls, written messages, etc. Indirect communication take the shape of information disseminated broadly to the public through statements geared toward the target, demonstrations of capability and commitment, and the publication of government-provided information in mass media outlets. During the Cold War, American and Soviet representatives frequently engaged in direct communication through diplomatic dispatches, telephone conversations, and through frequent official and unofficial meetings. But they also often engaged in indirect methods of communication - nuclear tests and televised military parades are good examples. Indirect communication is most useful in situations where a specific target of deterrence is unknown or there are no means of direct communication. It is also useful when obfuscating the communication source from the target, perhaps because of a high level of distrust between the target and the deterring party. Because of these two points, indirect communication is an important element of deterrence in the terrorism context. Indirect communication assumes that the target can and will receive information and messages provided through certain public media. Thus, information disseminated to the public can be designed for receipt by potential terrorists residing within the public.

Credibility

Deterrence involves a large degree of psychological interplay between the target and the deterrer. In large part, it revolves around shaping the perception of the target. If the target group does not believe the deterring party is capable of manipulating the costs and benefits in the course of responding to the action being deterred, the target will not incorporate the deterrer-provided information in their decision-making process. In other words, if the target does not believe the deterrer is either willing or able to respond as promised, information on what that response will be and how it will affect the actor will not influence the actor.

Credibility is an important, but challenging, conceptual element when attempting to implement a deterrence strategy in any context. It could be difficult for the deterring party to portray itself as credible when communicating with the target. The mode of communication may not be amenable to reinforcing credibility. Additionally, the target may not be willing to take any communication from the deterring party (especially when it is the United States government) as credible. For example, information purporting a high-level of terrorism preparedness in Washington or New York City can be perceived by certain actors to be part of a government misinformation campaign, and thus perceived to be a bluff. On the other hand, if the deterring party bluffs successfully, it will dissuade the terrorist without actually possessing the ability or willingness to manipulate costs, benefits, and risks as described.

Opportunities for Deterrence

How might policymakers successfully apply deterrence to counter CBRN terrorism? At what points will the instruments of deterrence affect the terrorist s decision-making process? Terrorism is not the moment at which a car bomb detonates or when salmonella bacteria sprayed on a salad bar begins to sicken restaurant patrons. Terrorism represents a series of interrelated activities progressing from ideology and value formation to the use of violence to support of the objectives of that ideology. Importantly, terrorism is more than a single decision to acquire and utilize an instrument of violence — regardless of whether it involves conventional explosives, nuclear devices, biological agents, or chemical agents. Rather, engaging in terrorism involves a series of decisions undertaken by a series of individuals (assuming the terrorist is not a lone actor) over an extended period of time. This fact is important to consider because the application of deterrence to terrorism involves attempts to influence each of those decision points and the individuals who carry them out. The following list of activities provides the basic process model for CBRN terrorism for this analysis. These steps are listed not in chronological order, but the order of logical progression. In other words, for each step in the model, the steps listed above that step must have previously occurred.

- *Ideology and Value Formation* - Creation of the group, individual, and individual affinity for group
- *Motivation* - Recognition of link between CBRN weapons effects and the group objectives, and the momentum driving to the actor to acquire and use CBRN weapons
- *Planning & Information Gathering* — Selection of type of weapon, identification and exploitation methods to acquire and develop weapon, and identification of potential targets
- *Acquisition* - Process of obtaining materials and equipment needed for weapon fabrication

- *Stockpiling* - Fabrication of CBRN weapon(s)
- *Deployment* - Preparing weapons for use (testing, evaluation, prepositioning)
- *Dispersal* - Actual use of the weapon
- *Exploitation* - Phenomenon resulting from use (mass casualties, fear & panic, political bargaining)

Instruments of Deterrence

While the basic elements of deterrence have not changed since the early days of the American-Soviet nuclear confrontation, the application of deterrence theory has changed according to changes in the threat environment. Even within the context of the Cold War nuclear confrontation, both parties adjusted the instruments of deterrence and the ways in which both parties employed these instruments in support of mutual deterrence, in response to technological improvements, changes in relative military superiority, and shifts in the international political environment. In the context of CBRN terrorism, the types of instruments and the number of instruments is broader than in the nuclear context. Like the Cold War, it includes communication, awareness, and punitive measures. Unlike the Cold War, both denial measures and defensive measures arefeasible and have utility within a deterrence framework.

Each of the following instruments could be used to exploit the opportunities for deterrence provided by the process of CBRN terrorism but no single instrument can in and of itself provide a robust CBRN terrorism deterrent. It is important to capitalize on the synergistic deterrent effect of the full set of instruments working toward deterrence.

Awareness

Awareness refers to the deterrer s ability to identify and assess both the target(s) of deterrence and the available opportunities. Apart from identifying and assessing targets and opportunities, it also supports the other instruments of deterrence by informing them or directing them toward their most productive application. Awareness incorporates a number of tools including traditional intelligence functions, law enforcement activities, open source information, and increasingly, information provided by non-governmental organizations involved with monitoring disaffected segments of society.

The process of identifying and assessing potential CBRN terrorists and the opportunities for deterrence can be broken into two levels, strategic and tactical. On a *strategic* level, awareness should identify the set of possible targets and provide key information on those targets, including some degree of understanding of motivations and value systems. Awareness can discern where costs and benefits can be manipulated, what the terrorist holds valuable including their perception of the utility of using CBRN weapon, ways to threaten what the terrorist holds of value, and the most sensitive points of leverage of a particular terrorist. This may include a fear of being discovered or punishment, loss of limited financial resources, or inability to achieve the level of violence perceived to be vital in achieving their objectives. Because much of this level of awareness involves understanding motivations, logic, and objectives, human intelligence is of particular importance. In addition to traditional human intelligence operations, potential sources include law enforcement activities, surveys and outreach activities completed by non-governmental organizations, and open source publications.

On a *tactical* level, awareness facilitates the instruments used for manipulation of costs, benefits, and risks. What are the possible threat agents and how should the country prepare for their use? What are the potential targets of attack and how should they protected? How is a suspected CBRN terrorist obtaining materials and equipment and what measures can be taken to prevent their acquisition? Answers to many of these questions require effective technical intelligence sources in addition to the human intelligence sources listed above. Answers to these questions also require a high-level of self-awareness. Assuming the terrorist will move down the path of least resistance, answering many of these questions requires continual surveys of internal vulnerabilities and capability levels.

Awareness also directly provides a means for increasing the costs incurred by CBRN terrorists. Recognizing the possible existence of an intelligence or law enforcement operation targeted at their activities, potential terrorists may find it necessary to take measures to thwart those operations, which may in turn increase the cost or disrupt their activities. They may also decide to skip entire steps in the process due to the substantial risk of discovery. In either situation, secrecy imposes a certain amount of cost on the potential terrorist.

A fundamental consideration at both the strategic and tactical levels of awareness is the integration, synthesis, and analysis of data from a multitude of sources. It is one thing to exploit various information sources to collect and then store information and data. It is another thing to use that data to understand the situation and provide both explanations and forecasts. The cornerstone of sound analysis is an intelligent, disciplined, alert analyst.

Denial Measures

Denial measures are designed to retard or completely prevent the acquisition of CBRN weapons, materials, equipment, and expertise by the terrorist. Many of these measures are economically oriented and serve to increase the cost of acquisition incurred by the terrorist. Costs are not only measured in terms of financial resources, but also in difficulty or ease of acquisition, expenditures of available time, anonymity, and the pesonal safety and security of group members.

Denial measures are designed to increase the cost and decrease the chance of success involved with acquiring or developing a CBRN weapon by complicating acquisition and development. Early recognition by the terrorist of the levels of difficulty involved should influence the decision to undertake subsequent acquisition activities before they are undertaken. A key ques-

tion is whether the terrorist can be dissuaded from attempting to acquire CBRN weapons through information on the degree of challenge and difficulty, and the low chance of success. Effective communication can serve to convey this message, but if our ability to control transfers of technologies to non-state groups is perceived by the terrorist to be ineffective, they are not likely to be deterred from attempting to acquire the requisite weapons, materials, and equipment. The key is shaping the terrorist s perception of the level of difficulty before
acquisition is attempted.

While bluffing may be part of policies supporting deterrence, actually increasing the level of difficulty associated with acquiring a CBRN capability will go a long way toward convincing potential terrorists that acquisition and deployment is too difficult. Many of the mechanisms and systems for controlling technology transfers to state actors are already in place at both the national and international levels. While they have been developed and refined to stem state proliferation, the regimes have dealt with front companies or illegitimate non-governmental scientific exchange organizations created by states to engage in illicit technology transfers. These regimes already attempt to address non-state actors, but they still need improvement to address the problem posed by non-state actors not linked with state programs. Legislation designed to regulate transfers of agents and equipment, stricter criminal laws, licensing for certain types of equipment, and allocation of resources to support implementation of these measures should be considered.

Defensive Measures

Policymakers have frequently touted the deterrent effect of robust defensive capabilities. How does defense translate into deterrence? Developing robust defensive capabilities before a CBRN terrorism incident can diminish or eliminate motivations for using CBRN weapons by mitigating their immediate impact - mass casualties, or the fear and insecurity that the use of such a weapon is likely to create. It is difficult to determine with any degree of specificity the mental interaction between motivations, weapon effects, and the longer-term objectives of a specific terrorist. It is fair to assume the potential CBRN terrorist is interested in this class of weapons rather than conventional weapons because of their potential for quantitatively and qualitatively higher levels of casualties, physical damage, and psychological impact. Preventing the terrorist from achieving their long-term objectives through the immediate effects of CBRN weapons can contribute to deterring the terrorist from both acquisition and use, and perhaps focusing their attention on potentially less destructive conventional explosives.

Robust defenses are most likely to deter acquisition and use of chemical, biological, and radiological weapons. Unlike nuclear or even conventional weapons, these three types of weapons are most amenable to defensive capabilities designed to mitigate the effects of their use.

Physical protective equipment donned prior to an attack can prevent both the physical and psychological impact the attacker is trying to achieve. Techniques to rapidly identify the agents, antibiotics, medical facilities, decontamination equipment, well trained medical personnel, shelters, filtered air, and evacuation procedures are just some of the physical protection measures against a chemical, biological, or radiological attack. In addition, the effect of these weapons is not the product of explosive energy with damage resulting from the blast and debris. It is the product of the released material s physiological effect on the human body. Because there is a delay between exposure to these materials and the onset of effects, a window of opportunity exists for agent mitigation and medical intervention. An effective defense against chemical, biological, and radiological weapons must also reduce the psychological impact. In large measure, having an effective defense capability in place before an incident will go a long way in calming the public fears both before and during an actual incident. Telling the public above the measures taken to prepare and respond will reduce anxieties. Counter-terrorism officials must also ensure counseling is available to deal with the psychologically traumatized casualties resulting from an incident.

The key to integrating defenses into a deterrence strategy is to make sure the target recognizes adequate defenses are in place before deciding to act. By informing the public and the potential terrorist of the nation s relatively low vulnerability to CBR weapons, the terrorist is more likely to conclude that the chance of meeting their objectives through the use of such weapons is low. In designing defense programs with deterrence in mind, the most important, but potentially most challenging question is how much is enough? More specifically, how much is enough to deter. Part of the answer depends on how much risk the terrorist can accept in deciding to act, in particular the risk of failure, and the amount of time and money the country is willing to spend to reduce vulnerabilities in a period of constrained budgets and competing priorities.

Punitive Measures

The objective of punitive measures is not to affect the terrorist s ability to obtain a CBRN weapon or effectively use it, but to impose high costs in response to attempts to acquire or use such weapons. Deterrence through assured punishment has always been a key component of deterrence strategies. While the application of military force can have a strong deterrent effect in theory, its contribution may be diminished in practice because force will not be an appropriate response to many CBRN incidents, especially minimal damage incidents, nor acquisition and development activities. When force is not an available instrument, effective law enforcement and prosecution plays an especially important role in punishing terrorists.

The deterrent effect of various punitive measures depends on the degree to which the potential terrorists value the group s survival, their individual freedom, and their individual safety. Punishment and retaliation will deter terrorists when the success and even survival of the group is jeopardized through the elimination of group members — either through arrest and prosecution of individual members or through the use of force against the group as a whole. Even if the potentiality of punitive measures has minimal deterrent effect on decisions made by the group s leadership, the possible loss of life and freedom may deter individual members from carrying through the group s plans.

Some individual actors, however, may not value their freedom and safety except insofar as it affects their ability to accomplish their immediate objective — acquisition and use of a CBRN weapon. These actors may not care about what happens to themselves or the group once the weapons have been used. In this situation, punitive measure will have a deterrent effect when law enforcement achieves a high-level of success in regularly identifying and prosecuting individuals attempting to acquire or develop CBRN weapons capability. Similar to the deterrent effect of denial measures, successfully identifying and prosecuting terrorists for attempting to acquire a CBRN capability will help convince future terrorists that acquiring this capability is too hard.

With respect to all possible means of punishment, law enforcement, prosecution, military force, etc., past actions seem to be important for shaping the terrorist s perception of the likely response to future attacks. As was mentioned previously, deterrence rests on the target s perception of the benefits and costs of acting before making the decision to act. Historical precedent does represent one piece of information the terrorist will use to make a judgment on acting or not acting, and the likely response to acting. Inaction in responding to previous terrorism incidents will adversely affect the deterrent value of punitive measures by decreasing the terrorist s perception of the likelihood that those measures will be taken in the future.

International Cooperation

Given the transnational nature of many terrorist networks and organizations and the potential for the effects of a CBRN terrorism incident to spread internationally, international cooperation is essential to ensuring that the other instruments of deterrence fully address the CBRN terrorism threat. Many of the previously mentioned instruments of deterrence currently exist but require some measure of adjustment to address the international dimension of this threat. For example, specific guidelines for sharing intelligence information could improve the capability to track and assess transnational terrorist groups. On the other hand, an international regime currently exists to address the state-to-state dimension of the proliferation threat, but may require some adjustment to address the non-state actor dimension of the problem. For example, only the Chemical Weapons Convention requires signatories to criminalize activities prohibited by the convention. In addition, multilateral agreements like the CWC, BWC, and NPT help to de-emphasize or even de-legitimize these weapons, thus promoting a social taboo against CBRN weapons. By itself, such a taboo contributes substantially to preventing incidents of CBRN terrorism.

Other areas for improving international cooperation to combat CBRN terrorism exist. While current export control mechanisms like the Australia Group are focused on the state dimension of the proliferation, other international mechanisms could help to regulate transfers of such items to non-actors and promote increased transparency regarding such transfers. Countries need to implement regulations designed to control the spread of biological, chemical, and radiological materials, like the CDC s Select Agent List and the recently introduced Dangerous Biological Agent and Toxin Control Act, on an international basis if they are to be effective. While such mechanisms are unlikely to eliminate transfers of technology, increased transparency will contribute to deterrence by increasing the cost of acquisition and increasing the risk of discovery.

In addition, greater international cooperation is needed to improve defensive capabilities on a global basis. The U.S. Department of State has been working with friends and allies in the Middle East and East Asia to provide counter-terrorism training in addition to providing detection and personnel protective equipment. In addition, the CDC is beginning to engage both nations friendly to the United States and international organizations like the World Health Organizations to improve global bioterrorism detection and response capabilities. These efforts are a good first step, but they must be expanded and multilateralized. As countries like the United States improve their own capabilities, they must cooperate with countries with similar levels of capabilities and assist countries with lesser-developed counter-terrorism capabilities. Without some degree of international uniformity in response capabilities, a high degree of preparedness in a country like the United States will deter the terrorist who has successfully developed a CBRN weapon from using it in that country, and use it in another. Such an incident will severely affect both American citizens and American interests abroad, and may affect the American homeland directly.

An important difficulty will be working with international partners while maintaining a unified message. Coordinating and sustaining both attention and effort will be difficult across international coalitions. Differences of opinion have developed within the United States over such issues as the precise nature of the CBRN terrorism threat, and the required response to that threat. Such disagreements certainly span international boundaries and could increase the cost and time required to foster international counter-terrorism cooperation.

Communication

As has been argued throughout this paper, the key to deterrence is dissuading the target from acting by communicating the likely or probable response. That response must serve three purposes: 1) increase the risk that the target will fail, 2) increase the cost the target will incur by acting, and 3) reduce the benefits the target hopes to derive from acting. To deter future acts of CBRN terrorism, the potential terrorist must be informed of the nature of the likely response to each of the steps in the CBRN terrorism process *before* the terrorist decides to undertake that step. The process through which the deterring party communicates with the target before he decides to act is central to providing the target with this information.

Government officials must identify and exploit available channels of communication with potential CBRN terrorists to provide a number of specific pieces of information. For each step in the CBRN terrorism process, messages provided to the terrorist must link the step with a specific response. They should also provide the terrorist with information on how the response will increase costs, decrease benefits, and/or decrease the chance of success, while shaping the terrorist s perception of both the ability and the willingness of the deterrer to respond as promised.

Exploited channels should include both direct methods of communication, if available, and indirect methods. If a specific terrorist is known and willing to listen, direct communication is possible and packages of information tailored for deterring the specific terrorist can be developed and disseminated. Because most actors will probably attempt to remain anonymous before attempting to carry out acts of violence, this type of direct communication with a terrorist will be unlikely in most situations.

In situations where a potential CBRN terrorist is suspected to exist but is not explicitly identified, communication is still possible through indirect channels. Because the potential terrorist resides within the public, mass communications, public relations, and various media outlets can be exploited to provide information to the potential terrorist. Some examples of this type of communication include broadly disseminated general statements (perhaps on the level of preparedness and defensive capabilities, the difficulty of acquiring or developing a CBRN weapon given the capability of various denial measures, and the high cost that will be incurred by the group and the individual members of the groups attempting or actually using a CBRN weapon) that filter through to the terrorist, use of third parties to provide information - either direct communication or general statements and declarations, intentionally providing a carefully calibrated level of transparency regarding high levels of current capabilities, preparedness, and vulnerabilities, open demonstrations of capabilities, and others. Transparency should make available a certain type and amount of information in order to inform potential terrorists about capabilities and preparedness, while not jeopardizing those capabilities in the process.

Because it is difficult to know if potential terrorists are listening to messages provided through indirect channels, a vital part of a communication strategy supporting deterrence is the identification of the specific channels to which terrorists are most likely to be open and determining the information requirements of the archetype CBRN terrorist. Planning a CBRN terrorism incident will require information on the level of vulnerability of a particular target, the type of security surrounding a target, or the type of defenses, for example the amount and types of vaccines included in the national pharmaceutical stockpiles. Much of the information terrorists require come from government sources, either directly or through third parties. Determining these requirements and the corresponding channels use to obtain that information may provide the opportunities to communicate with potential terrorists who have not been specifically identified, by providing a mechanism by which information can be provided to the terrorist.

The media is an important tool the government can leverage to support a deterrence strategy. This includes the print media, television, and the Internet. The government must carefully craft both the message and the medium used to communicate with the public and potential terrorists. Information provided to the public is likely to trickle down to the terrorist, for example, various statements by public officials to gradually expose the public to a new terrorist threat and gain its support in mobilizing an effective response. Through these statements, government officials may inadvertently communicate to the terrorist that developing and using certain types of CBRN weapons is easy or that we are highly vulnerable to such weapons (e.g., If it was difficult, it would not be such a large problem.) We will need to use similar statements, release official studies and evaluations, and conduct periodic demonstrations of maturing counter-terrorism capabilities to reduce public insecurities while deterring potential terrorists. During the Cold War, officials struck a delicate balance between transparency and opacity with regard to the nuclear forces of the United States. American counter-terrorism officials must strike a similar balance.

Conclusions

As this paper attempts to illustrate, it is possible to deter potential CBRN terrorists, but deterrence is not going to work in all situations for all actors. It is important to remember that the instruments of deterrence in the CBRN terrorism context are the same instruments that will be needed if deterrence fails.

The challenge facing policymakers lies in actively using these instruments to support deterrence in an integrated and synergistic way. Awareness will identify and provide understanding of potential CBRN terrorists. Awareness also supports the effective application of the denial, defense, and punitive measures. Effective denial efforts will reinforce the message that acquiring or developing a CBRN weapon is too costly or too difficult. Robust defensive capabilities deny the terrorist the immediate benefits of using a CBRN weapon — mass casualties and mass hysteria. Punitive measures impose a direct cost on the terrorist in response to attempting to acquire or use CBRN weapons. Given the borderless nature of the problem, international cooperation is key to ensuring the full effectiveness of the other instruments of deterrence. Finally, communication is a cornerstone of deterrence. Through effective mechanisms of communication, the deterring party can inform potential terrorists of the likely response, and do so before the terrorist decides to act.

It is important to recognize the relationship between various instruments of deterrence, especially the instruments that impact cost/benefit/risk manipulation. Perhaps the most important of these is the relationship between denial and defense measures. Successful denial measures should work to decrease the scope of the problem left to defensive measures to mitigate. A successful denial strategy will narrow the threat envelope, thus reducing the requirement for defensive measures. In other words, better denial measures will reduce the burden on defenses. Together, denial and defensive measures should be used to convey a message: it is too hard.

The instruments needed to deter potential CBRN terrorists currently exist, but policymakers and government officials need to integrate them into a policy framework specifically constructed to support deterrence. Within such a framework, communication plays a critical role. Through effective communication strategies, potential terrorists can be deterred from future incidents of CBRN terrorism by linking individual steps in the CBRN terrorism process to a response designed to deny benefits and increase costs, and thus influence decisions made by the potential terrorist in the present.

[1] The author would like to express his appreciation to Sandia National Laboratories, specifically Dr. Larry Brandt, for supporting the original study from which much of this paper has been generated. The ideas and conclusions in this paper are those of the author and are not necessarily endorsed by CBACI or its sponsors.

Biological Terrorism Variables and Emergency Response Concepts[1]

Richard W. Hutchinson, Ph.D.

Introduction. Biological warfare involves the use of microorganisms (bacteria, viruses, or fungi) or toxins to produce death or disease in humans, animals, and plants. This broad definition of biological warfare is in keeping with the essentially open-ended potential of such warfare with respect to target, timing, method of attack and agent employed. While use of the term "warfare" implies use in war between nations, vulnerability studies demonstrated the potentially devastating impact of biological weapons, should they be acquired and dispersed by terrorists.

Concerned about the Tokyo sarin-gas attack and the bombings of the New York City World Trade Center and the Oklahoma City Federal Building, Senators Nunn, Lugar and Domenici prepared legislation that called for improvement in domestic preparedness against terrorist use of chemical, biological, nuclear and radiological weapons. In support of this legislation, the U.S. Army Soldier and Biological Chemical Command initiated a Biological Warfare Improved Response Program to develop and to demonstrate improved concepts for responding to terrorist use of biological weapons against U.S. population centers.

To implement the program, a multi-agency, multi-disciplined team was formed to work through a series of realistic biological attack scenarios in order to converge on a practical system of response concepts. Realism of the attack scenarios was addressed through analogy to past U.S. biological simulant field-tests and by employing experts from the past U.S. biological warfare program. Practicality was achieved by including emergency responders, managers and healthcare providers within the team. This paper summarizes the insights gained with respect to the key variables of biological terrorism and the response concepts that were developed to deal with those variables.

Biological Terrorism Variables. Primary variables associated with biological terrorism are agent type, routes of infection, agent dissemination, residual hazard, and casualty dynamics. A short explanation of each of these variables is presented below.

<u>Biological Agents.</u> A key variable of biological warfare is the choice of agent. The Centers for Disease Control and Prevention (CDC) list anthrax, tularemia, smallpox, plague, filoviruses, and botulism as agents of greatest concern. Each of these agents was weaponized in state sponsored warfare programs with the possible exception of the filoviruses. Other lists of possible agents are much longer. The possibility of surprise- agents produced by terrorists or state-sponsored programs should not be discounted. Informative articles on a number of these agents are available on the Web (www.hopkins-biodefense.org/pages/agents/agent.html).

1. Disclaimer: The contents of this white paper are not to be construed as an official Department of the Army position unless so designated by other authorizing documents.

Considering the list of CDC agents as examples, what are the characteristics of these agents that would drive emergency preparedness concerns? Anthrax and tularemia are examples of lethal diseases that require prompt treatment to reduce death. In the case of tularemia, death can be greatly reduced if antibiotic treatment is initiated at the onset of symptoms. Conversely, anthrax requires antibiotic treatment before the onset of symptoms in order to avoid death. Thus, emergency response plans must include the ability to rapidly disburse pharmaceuticals to populations symptomatic or suspected of being exposed. Both of these agents are non-contagious and, therefore, the spread of disease from one person to another would not be a key concern.

Smallpox and plague are examples of highly contagious diseases that can spread from one person to another through the aerosol route. Patient isolation and immunization of family members and health care workers are critical concerns in responding to terrorist use of such agents. Smallpox is a virus and like most viruses with today s state of technology, is untreatable once symptoms appear. Plague is also a highly lethal disease, but it is treatable before or at the onset of symptoms.

Other possible agents such as Venezuelan Equine Encephalitis (VEE) and the toxin SEB have a very low lethality though they produce severe illness. VEE is a virus for which there is no treatment.

For all of these agents, the virulence of the particular strain employed will impact the number of casualties produced during a particular incident. For example, the Japanese cult Aum Shinrikyo used a vaccine strain of anthrax in their attempted attacks on Tokyo and failed to produce any casualties.

In summary, biological agents can be characterized as lethal or non-lethal, treatable or non-treatable, and contagious or non-contagious. These characteristics drive emergency preparedness with respect to availability and distribution of pharmaceuticals, isolation of victims, and plans for handling large numbers of diseased. Thus, rapid identification of the agent following an attack is paramount. For all of these diseases there is the need to provide supportive care of the victims — however many that may result from a particular attack. The diseases caused by known biological agents are severe — more intense and debilitating than the usual flu.

Routes of Infection. The primary routes of infection for biological agents are through aerosol inhalation, ingestion and skin abrasions. The aerosol route is of greatest concern because of the potential to infect large numbers of people such as in a subway or a sports arena. The outside release of biological agent as a "line source" could potentially infect a large population center. Contamination of food at a restaurant or food processing plant is another approach that was demonstrated in Oregon by the Rajneeshees in 1984. Cutaneous anthrax is an example of infection that can occur through skin abrasions.

From a response perspective, the first indication that a biological event has occurred will probably be the presentation of sick people to clinics and emergency rooms regardless of the route of entry. Most biological agents have an incubation period of one or more days before symptoms appear. The route of entry is important to epidemiological investigation in order to identify the population at risk. It is also important to criminal investigation in order to project backward in time to the release location and source.

Agent Dissemination. Biological agents may be dispersed as an aerosol using an explosive device such as a charge inside a container of liquid agent, a spray device for liquid or dry powder agent, or through natural dissemination such as the dispersion of a dry powder in a subway. Dry powder agent is the easiest to release and can have an aerosol efficiency of 20% or higher, but it is the most difficult and hazardous form of agent to produce. Explosive devices usually have aerosol efficiencies of less than 0.1%, and liquid spray devices have intermediate efficiencies. Aerosol efficiency, as used here, refers to the percent of infectious organisms released into an inhalable aerosol of 1 to 5m in diameter. Release of a biological agent at a low efficiency means that most of the infectious organisms are contained in large particles which fall to the ground close to the release point. The successful release of a biological aerosol is not trivial. The Aum Shinrikyo of Japan was not successful in infecting anyone in their attempts to disperse biological organisms.

The following table shows key aerosol parameters that relate to biological warfare. Particles of 1-3m deposit in the deep lung where they are most effective in causing disease. Also, the small particles settle slowly and, therefore, stay air-born for a period of hours giving opportunity to infect many people over a wide area. The larger particles settle much faster and thus are quickly removed as an inhalation hazard. Further, large particles deposit in the upper-respiratory track where they are less likely to cause disease.

[Figure: SEE ATTACHED FILE]

The wide range in efficiency of aerosol release that terrorists of varying capability might achieve could impact emergency response in the following way. A given target attacked with a highly concentrated, efficiently dispersed agent could produce infection in 90% of the target population. If that same target were attacked by a dilute, inefficiently dispersed agent, only a small fraction such as 1% of the target population might be infected. Thus, the scale of the biological attack cannot be directly equated to the number of people exposed; rather it is a combination of the target population and the efficiency of attack. Since the efficiency of attack will in all likelihood be unknown, response should focus on the number and location of victims ascertained through epidemiological investigation.

Residual Hazard. Aerosol particles that deposit on surfaces following the initial release do not generally pose a serious residual hazard for the following reasons. First, it is the large particles that deposit in high levels close to the point of release. These particles do not tend to re-aerosolize in the inhalable range where they would pose an inhalation hazard. Second, the fine particles settle in low concentration over a wide area because of their low settling velocity. After settling, they adhere strongly to the surfaces. Consider how fine dust adheres to a windshield at 50 mph. Therefore, the fine particles tend to be re-aerosolized in very small numbers, and thus produce a minimal hazard. Further, between the time of the biological attack and the onset of casualties, the agents on surfaces would undergo biological decay that would also reduce the residual hazard.

While a secondary aerosol hazard is not likely to produce additional casualties, there is the possibility that some of the bulk agent could be left in the device or close to the release point. If this material is a dry powder, it could pose a residual hazard. Thus, there is uncertainty regarding residual hazard following a biological attack, and protection would be warranted in collecting evidence at the release site.

Casualty Dynamics. Victims of a biological aerosol attack will be exposed almost simultaneously. As a result they will become ill within a compressed period of time. Casualty curves for anthrax are shown in the following figure. Following exposure, no casualties would occur for at least 24 hours during the incubation period. Then, a few people would become ill with flu-like symptoms. These would include exposed people that were immune depressed and those that received an exceptionally high agent dosage. During day three the number of people becoming ill would increase dramatically, and a few of the infected would progress to the critically ill stage. During day four, fatalities would begin to occur, and the number of critically ill would greatly increase. Sometime during day 3 and 4 the media, the public, and the health care and emergency response community would become aware that a medical emergency was underway. Then, the number of worried well seeking medical care would be a multiplier of 5-10 times the number of ill seeking medical care as was observed in Tokyo following the nerve-gas attack on their subway. These curves would remain essentially the same for any scale of attack because everyone would be exposed at the same time regardless of the scale of attack. In the case of contagious diseases, additional secondary and tertiary infection waves would occur unless steps were taken to contain the outbreak.

[Figure: SEE ATTACHED FILE]

The curves shown here represent a high level of exposure. Casualties resulting from a low-level release of anthrax spores over Sverdlovsk Russia presented over a more extended period. For other agents, the set of curves would move to the left for diseases with a shorter incubation such as VEE or to the right for diseases with longer incubation periods such as smallpox. The fatality curve would greatly diminish for non-lethal diseases, and the critically ill curve could extend further to the right.

The dynamics with which casualties occur following a biological attack is a key driver of emergency response concepts. Detection and identification of the disease is likely to occur during days 3 or 4. By that time the numbers seeking medical care and the critically ill would be on a steep rise and would peak within one to two days. Anything that could shorten the time to detection and identification would give more time to cope effectively with the rise in casualties. But even under the best of circumstances with early detection, the rapid increase in casualties would imply the need for a local-based response system in order to keep pace with casualties resulting from a biological attack.

A second key factor driving the response is the number of casualties. These curves are scaled for a large and efficient biological attack against a large population in a subway, a sports arena, or a metropolitan area. This same attack, but with a dilute agent inefficiently disbursed, might produce 1,200 or less casualties. The scale of a biological attack cannot be predicted beforehand. A robust response strategy must be able to cope with a very wide range in numbers of casualties.

Summary, Biological Attack Variables. Variables associated with possible biological attacks include choice of the agent, method of dissemination, route of infection and selection of target and times. From an emergency response perspective, these unknown and uncontrollable variables would all manifest in the presentation of sick and worried people that must be calmed, treated, given supportive care, and possibly handled as fatalities. The unpredictable scale of biological attacks makes it possible that local medical capabilities would be overwhelmed. The dynamics of casualty presentation necessitate rapid detection and identification, and very rapid response. Uncertainty regarding residual hazard implies the use of protective measures in collecting evidence.

Coupled with these variables is the overall uncertainty of the biological threat. We might think of biological terrorism as a potential peril that could become an immediate peril quickly, with little or no warning, and with devastating impact. Faced with this possibility, two choices are evident: (1) Prepare before the event; or (2) Prepare after the event. We do not know if a biological event of devastating proportions will ever occur, but that fact does not alter these two choices. If we do choose to prepare to respond before the event, the low likelihood that such an event would occur in a given locality does have a practical impact on response strategy. A response strategy needs to be both effective in coping with a wide range of biological attack variables (or it may fail) and practical with respect to cost, effort and simplicity (or it will not be implemented).

Emergency Response Concepts. To develop concepts for responding to a biological attack, a 60 member multi-disciplinary team of local, State and Federal emergency responders and managers, and technical experts analyzed five attack scenarios during a series of five workshops. The sequence of scenarios was as follows: an attack on a building with tularemia infecting 1,000 occupants; an attack on a sports arena with a mixture of SEB toxin and tularemia infecting 20,000 attendees; an attack on a subway with anthrax infecting over 100,000 riders; and an attack on a metropolitan area with VEE virus infecting over 1 million residents. Finally an attack on a cattle feed lot with Rift Valley fever producing illness in both cattle and humans was analyzed. The scenarios supported by tutorials on key aspects of biological warfare not only provided examples against which to develop response concepts, but also served to establish a common basis of understanding of the nature of the biological warfare.

After presenting each scenario, the team was asked to identify the response activities that they would take and timelines of when these activities would need to occur. Response concepts resulting from the first two workshops were incomplete — approaches to deal with the large number of casualties had not been identified. However, in the third workshop the team built on what was learned from the first two workshops and produced an integrated concept for dealing with a major biological incident. The team also estimated the resource requirements to implement the concepts and then identified available resources to fulfill the requirements and shortfalls. During the fourth workshop the response strategy from the third workshop was re-tested and strengthened, and the resource estimates were refined. The process was repeated again in the fifth workshop by applying the response strategy to an agriculture target.

Response Strategy. The key aspects of the resulting biological response strategy are the following.

1. Emergency response plans need to be integrated at local, State and Federal levels and in place before the event.
Reason: Responding to a sizable biological attack will require additional resources from State, regional and Federal levels that can be most effectively utilized if they are integrated into the planing. Given the complexities and time constraints of responding to a biological incident, trying to determine roles, missions and strategy during the event would likely fail. Consistency of response concepts throughout the nation would greatly facilitate the efficient application of outside resources whenever and wherever they might be needed.

2. Response to a biological attack needs to be locally based.
Reason: Rapid response is necessary to keep pace with the casualties. The local community, which understands its own needs, resources and population base, is in a unique position to respond rapidly and to provide a framework for quickly absorbing and effectively utilizing outside aid.

3. Response concepts need to prepare for a wide range of casualties.
Reason: The scale of a biological attack cannot be predicted. A terrorist biological warfare attack has the potential of infecting from several individuals to 10% or more of a locality's population.

4. The primary focus of the response needs be on care of casualties, worried well and those at risk. Plans to expand local medical capabilities need to be in place with pre-established lines of communication. Use of outside and non-traditional resources over a protracted duration needs to be anticipated.
Reason: Coping with the large number of casualties and worried well is the most difficult aspect of biological response planning and, therefore, requires special attention.

BW Response Template. In fulfilling these aspects of the response strategy, the team grouped response activities to provide structure and organization to the response concept. The resulting integrated response strategy is depicted as the BW Response Template in the following diagram. Key decisions that health and local officials would need to make during an emergency response are also indicated.

Continuous surveillance is an ongoing activity to monitor available information such as emergency room visits and ambulance runs for unusual levels of activity. These non-specific indicators can draw attention sooner, rather than later, that an unusual health event is occurring. The CDC now has grants to States and localities to develop and to test approaches for continuous surveillance. Such surveillance would assist in the early detection of both natural and terrorist spread disease.

Should continuous surveillance give indication of an unusual occurrence, surveillance would be immediately expanded by actively polling emergency rooms, clinics, doctors offices, veterinarians and others to better define the extent and nature of the medical situation. If expanded surveillance gave indication that a major or unusual health event was occurring, then medical diagnosis and epidemiological investigations would be implemented to determine the cause and to identify the population at risk. Criminal investigation would be started at that time to help determine if the disease outbreak was the result of malicious intent. Epidemiological and criminal investigations could usefully share information, as both investigations would be striving to identify the nature and site of the attack by interviewing casualties. Epidemiologists seek information to better define the population at risk, and criminal investigators need the same information in order to know where to look for evidence.

During the course of these investigations the number of ill and critically ill would be building. There would be enormous pressure on local officials to make decisions regarding prophylaxis, treatment, isolation and appropriate emergency response. It is likely that these decisions would be made on a presumptive basis within 12 to 24 hours after expanded surveillance indicated that a major public health event was occurring. Efforts to confirm medical diagnosis, refine the estimate of population at risk, and expand criminal investigation would continue, and the ongoing emergency response would be altered as needed based on the new findings.

The lower nine elements of the response template address the emergency response activities. Hazard assessment, mitigation and control would address residual hazard at the site of release and include control of contaminated food and vectors should these be applicable to the situation. Prophylaxis, immunization and care of casualties form the core elements of the response template. These elements must deal with the large numbers of both victims and worried well. It is through these elements that existing local medical capabilities would be expanded to form a system into which outside and non-traditional resources could be absorbed and utilized. To this end, the team developed the concept of a modular emergency medical system. The key components of this system are shown below.

Neighborhood emergency help centers or points of distribution would be established to provide prophylaxis, immunization, and information to those seeking medical aid. The centers would also triage incoming patients to separate the critical ill for transportation to other facilities. One concept is to expand existing clinics with volunteers and administrative staff to allow for a throughput of 1,000 patients per day or greater. Alternately, the centers could be established in other temporary facilities such as hotels. Acute care centers, which could satellite off of area hospitals, would provide treatment and supportive care for the critically ill that exceed hospital capacity. These would depend on a skeleton staff of local physicians and nurses augmented with volunteers and outside state, regional and federal medical personnel.

A complementary approach is to allow the critically ill to stay at home. Medications would be provided at the home, and family members, volunteers and outside medical personnel would provide supportive care. Community outreach would be necessary in most cases because some victims would not be able to access a neighborhood help center or other assistance. Recent analysis of attacks with a contagious disease organisms indicated an advantage if the ill are kept at home for purposes of isolation. Taken together, these three components offer flexibility in dealingwith large numbers of casualties resulting from a biological emergency. However, they would only be effective if the local health care community worked together as an integrated system under centralized command and control during such an emergency.

Key Components,
Modular Emergency Medical System

[Figure: SEE ATTACHED FILE]

Control of the affected area and population would involve both public information and security at health-care facilities and other vital installations. These activities are directed at calming the public and obtaining public support and compliance with the response measures as well as maintaining order and calm at health facilities. Resource and logistic support would focus on receiving and employing outside aid to include both medical supplies and personnel. Receiving and credentialing points would be needed for incoming medical personnel and volunteers. Logistic supply centers would be needed to receive, divide and distribute supplies.

Continuity of infrastructure may require public utilities and other critical services to implement their emergency operation plans if their staffs are reduced as a result of the attack. Distribution of prophylaxis to key utility workers could be required depending on the circumstances. Fatality management involves plans to augment the staff at local morgues to increase the processing rate and to use refrigerated facilities or vehicles as temporary fatality storage sites pending final disposition. Family support services are needed to provide information and assistance to the families of emergency responders during the incident as well as to deal with the longer-term psychological impact of the incident.

Command and control at the local, state and federal levels is needed to tie all elements of the response together. Local command and control would focus on coordinating the emergency response. State and federal command and control would focus on supplying outside support. Although a biological terrorist attack would result in a catastrophic medical emergency, and the medical community is paramount in deciding on the nature of the disease and treatment regimes, it will fall on the emergency managers to make the various response elements work together and to call for and integrate outside resources. Effective response to a biological incident would only occur if these two communities worked together in an integrated fashion. This integration would need to be pre-planned before the event and lines of communication would need to be pre-established. Additional information is available at Web location www2.sbccom.army.mil/hld/ BW Improved Response Program "Interim Planning Guide for Improving Local and State Agency Response to Terrorist Incidents Involving Biological Weapons."

Conclusions. It appears that effective response to a biological incident would be possible through pre-planning and preparation. Further, the cost of such preparation for a given locality appears modest since the main activities are planning and establishing lines of communication. The addition of costly local infrastructure is not necessary. The cost of continuous surveillance, the only ongoing element of the response template, appears modest since it involves the capturing and analysis of already existing data. At the Federal level, one of the main costs in preparing to respond to biological incidents is the need to stockpile antibiotics and vaccines. The CDC is currently establishing a national pharmaceutical stockpile.

Preparations for a biological emergency would be applicable to any catastrophic medical emergency that could result from natural epidemics, earthquakes or hurricanes. Thus, there is side benefit in preparing for biological incidents that would help the medical and emergency communities respond to other more likely medical incidents. Further, emergency managers have noted that many of the elements of the BW response template would be applicable to many natural emergencies.

Preparing to respond to a biological incident is not a simple task. Emergency managers and health care officials are already faced with a wide array of emergencies with which they have to cope. Taking the time and energy to plan for a low-probability biological event poses a difficult question in terms of priority. To assist localities in implementing the response template, a computer program is being developed called the response assets management system (RAMS) that will provide the BW response template in a convenient computer-based form. Equally important, it will assist emergency managers on a day-to-day basis with scheduling and time-keeping. The automated format will also allow response templates to be stored for other types of more routine emergencies. Thus, RAMS will provide the ability to automate local emergency response plans, which can then be shared as best practices between communities. The approach has potential to not only help implement biological response planning, but also to improve emergency planning and response throughout the country.

A final insight: it appears that the best response to a biological incident may reduce death, suffering and economic loss by approximately 50%. This level of saving would be of enormous benefit and would seem to justify improving response preparations. However, the remaining level of loss would still be enormous and totally unacceptable. Thus, biological terrorism must be prevented.

MEDNET: A Medical Simulation Network Grand Challenge

Michael Myjak, M.S. and Joseph Rosen, M.D.

Keywords: Advanced Distributed Simulation (ADS) DIS Telemedicine HLA

Abstract - The need to improve war-fighter training led to significant advancements in simulator technology. Now, simulator technology is ready to be applied to a new challenge: an evolutionary approach to training military medical personnel that will result in improved combat casualty care. With the exception of the introduction of helicopter evacuation support during the Korean War, changes in combat casualty care have not significantly altered the percentage of wounded soldiers lost in combat since World War II. The introduction of battlefield simulator training has improved strategic planning and combat readiness. It is time to apply these same tools to improvement of medical planning, military medical readiness, and execution of casualty care.

1.) MEDNET - An Overview

The MEDical simulation NETwork (MEDNET) is envisioned as a comprehensive simulation system that can be used to augment combat casualty care, support civilian medical training, and to provide just-in-time basic first-aid training in the event of terrorist attack. Viewed as a Grand Challenge for improving military medical readiness and combat casualty care, MEDNET is anticipated to become a fully integrated part of the overall strategic training mission of military medical personnel.

The challenge before us is the integration of a number of existing and evolving simulation and medical technologies. The concepts behind MEDNET are based on the blending of Advanced Distributed Simulation (ADS) technology and modern, emerging telemedical technology. ADS technology includes enhanced Distributed Interactive Simulation (DIS), as well as constructive and live simulation capabilities. In support of ADS, the Institute for Electrical and Electronics Engineers recently approved a simulation interface standard [IEEE 1516] known as the High Level Architecture (HLA). The HLA is sponsored by the Defense Modeling and Simulation Office (DMSO).

Based on the HLA standard, MEDNET could enable the simulation of any number of events and environments including, but not limited to, civilian patients, wounded combatants, patient surroundings, and the various echelons of care. In addition, MEDNET could leverage Internet technologies to incorporate a virtual clinician to provide support in diagnosis and disbursement of general medical knowledge to both medical and non-medical military or civilian personnel.

To date, biological weapons have not been used. However, in the unlikely event of a widespread biological threat such as unforeseen terrorist activity or a natural outbreak of disease, having MEDNET available to provide assistance to non-medical personnel may save a significant number of lives. Biological weapons are strategic in nature, and often spread well beyond their intended target (i.e., the Dandelion Effect). Should a biological threat occur, quarantine measures will no doubt be implemented and communications media (e.g., telephone, radio, and networking services) will become critical assets in fighting such terrorist activities. MEDNET, perhaps as an extension to the Health Alert Network, can play a role in supporting the transmission and communication of medical information and operations to combat the biological threat over a widely distributed communications network.

Recent advances in World Wide Web technologies and applications, continuous performance improvement in computing and communications hardware, and the continued evolution of the Internet-2 and Next Generation Internet indicate that future bandwidth will be available to support and sustain a geographically dispersed, distributed simulation system. In the following sections, we will describe the various components of MEDNET.

2.) The Components of MEDNET

The concept of MEDNET is based on existing distributed and reconfigurable simulation system technology suitable for both individual and team training. The primary components of MEDNET include the ADS system (the core of MEDNET) and infrastructure, the virtual patient simulator, a fully immersive 3D rendering system, an injury catalog database incorporating a comprehensive library of known branched-physiological scenarios, and an adaptive intelligent interface module called the Virtual Clinician Assistant.

Using the components of MEDNET, future civilian and military medical personnel will be able to educate and train in a synthetic environment (e.g., surgical theater, urban street accident, battlefield, rural area, etc.), triage and treat virtual injuries, and seek expert guidance, all from within the virtual environment of MEDNET. From a portal on the World Wide Web to a fully immersive virtual environment, MEDNET will be capable of offering a wide range of educational and training capabilities. The Grand Challenge of MEDNET is to provide this vast array of capabilities in a cohesive system that also supports differing levels of detail.

At one end of the spectrum is MEDNET's Web Portal Interface. Through this interface, MEDNET has the capability of providing basic first aid information to a broad constituency, such as the general public. In an operational setting, MEDNET has the capability to support JIT communications and operations support. In instances of terrorist attack, hundreds of thousands of people are going to want to know where to turn for general first aid information, assistance, or

quarantine rules in the event of a biological threat. In the latter example, we now know that local and regional hospitals and trauma centers become quickly overloaded when the number of injured reaches O(100). In fact, a recent simulation (a socratic dialogue) sponsored by the Institute for Security Technology Studies at Dartmouth last July indicated that health officials may be unable to triage the vast majority of the injured public. Further, as the first responders are the second to fall, the system is expected to collapse rapidly. Then where will people turn for basic information and first aid? The answer is the Internet. And where on the Internet will they be able to find up-to-the-minute information in an on-going crisis?
MEDNET.

At the other end of the spectrum is MEDNET's fully immersive environment. In its fully immersive capability, a virtual reality (VR) cave would be constructed around modern data-grade video graphics projectors, suspended from the ceiling and displaying on four surrounding walls. The expectation of this system is that this simulated synthetic environment will render a 360-degree field of view that fully immerses the participant(s).

In the center of this rendered space resides a table (a high definition volumetric display) that will present the virtual patient image to the interactors. This display presents a stereoscopic image that appears as a scale model resting on a table, gurney, or litter. The interactor(s) may view this image from any angle by walking around the table or by leaning over it to gain perspective from various azimuths and altitudes. Perhaps of particular interest are the data fusion capabilities of this display, which integrate graphical or multi-dimensional datasets with the virtual patient display. A true synthesis of MRI, 3D ultrasound, or other CT data can be used to morph the virtual patient to simulate a particular patient condition. When merged and morphed with data from the Visible Human Project, a true-to-life rendering is produced. But the grand challenge goes even further simulating the entire patient electro-mechanically, chemically, biologically, etc.

3.) The Virtual Patient Simulator

At the center of the MEDNET synthetic environment will be the high fidelity Virtual Patient Simulator (VPS). The VPS is the subsystem responsible for modeling and rendering the human patient form in considerable detail. The core of the human model used by MEDNET could initially be constructed using a blend of ADS technology developed by the U.S. Department of Defense and the Visible Human project from the National Institutes of Health. However, there is little reason to stop there. There are many systems and processes that can be modeled, both independently and in synchronicity with other systems. Theoretically, this could take us down to the operational level of DNA, or to as high of a level as bedside manner JIT Training. The challenge is both research-oriented and educational.

There are many ways in which a human patient simulator could be used. For example, scenario-specific data for a virtual patient simulation could be initially drawn from a physiological patient database. Then mathematical behavioral models contained within the injury catalog could be selected to create a scenario-specific medical event, possibly from stored Magnetic Resonance Imaging (MRI) data sets. These displays could then be superimposed on the digitized Visible Human and *morphed* as appropriate onto a standard human model. Visual or *polygonalized* data collected from the National Library of Medicine's Visible Human project could then provide a texture mapped overlay to generate quite realistic imagery. In another example, the virtual patient-generated image might contain generic ADS entity models. It may be possible to extend this presentation (such as in a learning environment) by synchronizing and registering a live data fed and superimposing it on the simulated patient. Given that livepatient information is being collected (e.g., x-ray mapping) and displayed in the surgical theater today, this part of the challenge is the next logical step.

In most technical training environments, immediate assessment and feedback on performance can greatly enhance the task acquisition process.

Initial VPS systems will likely be a composite simulation system (a blend of live, real-time, and constructive simulation technology) utilizing an aggregation of both low and high fidelity modeling techniques. Low fidelity modeling will be accomplished using constructive simulation techniques. When aggregated with virtual simulations, the VPS will be used to manage the majority of the patient's sub-systems in a logical and coherent fashion. High fidelity modeling that requires a high-degree of interaction will be accomplished strictly using real-time distributed interactive simulation techniques. Today, multi-processor-based systems are capable of providing the high-degree of interaction and fidelity required to train a clinician or medical corpsman. What's missing is the human patient simulation.

4.) The Haptic Interface

Human-computer interaction has historically consisted of limited interaction with visual displays of iconic and character data on a two-dimensional screen. Networked Virtual Environments (Net-VEs) offer an alternative interaction paradigm in which users are no longer simply external observers of data but are active participants with their data in a 4D virtual world. Within the Net-VE, force sensation plays an important role in recognition of 4D objects and our interaction with them. The hardware and software technology involved in the creation of interactive virtual environments such as MEDNET is still relatively new; however, haptic devices are already available in commercial-off-the-shelf form.

A high fidelity haptic simulation of surface contact presents a demanding technical challenge in the design of force reflecting Net-VEs. In fact, the creation and quantification of the characteristics of each of MEDNET's application components is a research task in itself. One of the main objectives of the MEDNET Grand Challenge is to stimulate research. This includes the identification and quantification of representative force sensations by an interactor in the 4D synthetic environment.

[Figure: SEE ATTACHED FILE]

Figure 1 High-Fidelity MEDNET Simulator Configured for Surgical Training.

Surrounding the volumetric display within MEDNET will be a set of haptic (tactile/force-feedback) interaction tools. These tools that comprise a technology assessment will permit the interactor to reach out, touch and *feel* the VPS. The haptic systems in MEDNET that permit the interactor to touch, feel, and otherwise physically interact with the VPS will lead to evaluation and characterization of the fidelity necessary in haptic devices and the human factors associated with tactile and force-feedback systems in medical simulation applications.

High fidelity, distributed interactive simulation techniques will provide for adequate *man-in-the-loop* interaction and response times. Although direct feedback to the interactor will be provided for by the haptic system, interaction and rendering will be controlled by the distributed Net-VE. Entity-to-interactor interaction will encompass various surgical tools and simulated telemedical instruments. Additional techniques can be programmed into the MEDNET system as new tools are added to support a variety of training and educational tasks.

5.) Three and Four Dimensional Displays

In many applications, the understanding and interpretation of visual images are inherent parts of the problem solving process. Examples in medical imagery range from diagnostic radiology and fluid-structure interaction to problems involving operator-assisted telerobotics. In MEDNET, the computer can be used to perform image, data, and knowledge processing in a way that is aligned with an understanding of the user.

Pseudo-holographic display systems can enhance our understanding and interpretation of visual images. They also provide for more realistic imagery. For the interactors, this display system can enhance interaction with the virtual patient simulation and further the immersion effects. In addition, several different levels of medical clinicians can be trained using MEDNET's reconfigurable environment. Clinicians can perform physical assessment tasks and practice procedures.

The objective of these systems is to provide high-fidelity video stimuli to the trainee with a minimal amount of distortion. This can occur in the VR Cave, or through the desktop using LCD shutter glasses. This can enhance the realism associated with the actual simulated environment. While this appears feasible and sensible on the surface, little research has been done to verify training effectiveness, cost effectiveness, human factors, or the impact of display system types. Network performance and training effectiveness are particularly troublesome and limited. However, initial system prototypes do appear quite promising, and recent assessments by the Army Research Laboratory appear to support the claim that interactors using 3D visualization appear to perform at a superior level to those using only 2D visualization. Thus we have good evidence to lend credence to the belief that 4D interaction may indeed be superior still.

6.) The Virtual Clinician Assistant

A significant amount of research has been conducted in developing techniques for embedded assessment for intelligent tutoring systems. This area focuses on the application and extension of real-time embedded assessment technology to casualty care. Today we believe that this level of assessment could now be integrated with modern knowledge-base technology and made available to the public at-large through the Web.

Consider that in most technical training environments, immediate assessment and feedback on performance can greatly enhance the acquisition process. This is especially true for procedural based applications (e.g., diagnostics, control procedures, etc.). When procedural errors are identified in real-time, it is easier for the learner to comprehend the context in which the error occurred. Often it is the situational variables that lead to a procedural error, hence corrective feedback in real-time aids in learning to avoid situationally induced errors.

The Virtual Clinician is the focus of research on the development of a prototype real-time intelligent embedded assessment module that would be integrated with MEDNET. This module would capture the procedural knowledge for a selected subset of diagnostic and/or operational activities. This involves knowledge engineering of selected procedures, development of the prototype knowledge model, and integration and testing of the Virtual Clinician interface. Further, timely information could be programmed into this interface to provide Just-In-Time training to the public at-large.

One of the side benefits of a validated embedded assessment module is that it reduces the number of live assessment experts needed for training. The Virtual Clinician prototype will be structured so that it can be extended into a comprehensive model in the out-years of the MEDNET program. This is perhaps by far the most visionary component of MEDNET.

A key element necessary to enhance many of the tools and models being developed is the need for an intelligent diagnostic aid. The intelligent diagnostic aid would exploit neural network technology, specifically back propagation neural networks, to provide expert diagnosis based on selected physiological scenario inputs. This type of expert systems approach is vital to the development of medic and physician-centered training. A fundamental reason for the importance of this type of system to the long-term goals of the MEDNET project is the same as for any expert system, the retention of expert knowledge.

Often the time between armed conflicts is lengthy. As a result, each time the military enters an armed conflict, it has a staff of physicians and medics with little or no direct experience in combat casualty care. The objective of the intelligent diagnostic aid within MEDNET is to create a system that can capture combat casualty diagnostic knowledge so that it is permanently archived and accessible during future training and conflicts. Later, this knowledge can be moved into the civilian sector to aid in diagnostic training and emergency room care.

7.) Conclusion

A grand challenge is a feat no one has attempted, but one in which we can see how it could be accomplished. MEDNET is one such grand challenge. This challenge will generate an immersive and highly adaptable virtual environment that will allow individual participants or teams to train simultaneously. The scenes presented within the MEDNET cave can change from a front line battlefield, through combat support hospital, all the way back to a remote hospital located in rural New Hampshire or urban Miami. Indeed, the entire continuum of support echelons can be modeled. Modeling treatment received prior to, during, or after transportation, or post-operative care can be but one focus of MEDNET simulations. Situational awareness training garnered through each step in the design of the 21st century medical system will be supported.

This integrated use of MEDNET, coupled with the World Wide Web and Health Alert Network represents a training simulation of providing casualty care as a comprehensive and realistic simulation exercise. Further, as our communication infrastructures stabilize and evolve, there is every reason to believe that a training system such as MEDNET could also be used in an operational capacity. The MEDNET training environment will therefore be a knowledge delivery environment, enabling medical personnel to better understand and manage the toll exacted by casualties.

About The Authors

MICHAEL D. MYJAK is Vice President of Research and Development, co-founder and Chief Technical Officer of The Virtual Workshop, Inc., where his current role is as chief architect of *JAVELIN*, a Java-based Run-Time Infrastructure for the Next Generation of Internet applications. In 1982, Mr. Myjak received two Bachelor of Science Degrees from Clemson University, one in Computer Science and the other in Engineering Technology. He obtained his Master of Science Degree in Computer Science - Systems from the University of North Texas in 1988 while employed with the Computer Science Laboratory, Corporate Research and Development labs at Texas Instruments. Prior to founding The Virtual Workshop, Mr. Myjak was a Senior Research Scientist with the Institute for Simulation and Training, at the University of Central Florida where he continues to teach *Building Virtual Worlds.* Mr. Myjak has been an active participant in Modeling and Simulation standards activities for a number of years, and was recently re-elected as Chair of the Standards Activity Committee (SAC) of the Simulation Interoperability Standards Organization (SISO). He has previously Chaired the Run Time Infrastructure and Communications Forum and the Run Time Infrastructure Interoperability Study Group under SISO, and the Internet Engineering Task Force's (IETF) Large Scale Multicast Application (LSMA) working group. Mr. Myjak is active in the Web 3D consortium's Virtual Reality Transfer Protocol Working Group, and the Internet Research Task Force's Reliable Multicast Research Group.

Doctor Joseph M. Rosen is an Associate Professor of Plastic and Reconstructive Surgery and an Adjunct Professor of Radiology at Dartmouth Hitchcock Medical Center in Lebanon, New Hampshire. In addition, he is an Adjunct Associate Professor and Lecturer at Dartmouth's Thayer School of Engineering, where he teaches a class on Healthcare Technology in the 21st Century, and is also Associate Professor of Surgery at Dartmouth Medical School. As well is a staff surgeon and director of the Plastic Surgery Residency Program at Dartmouth-Hitchcock Medical Center. His research interests include microsurgery and transplantation of limbs, nerve repair, computer-aided surgery and virtual reality simulators, and methods of education. In addition to his clinical and research activities, he has served as an adviser on public policy involving medical technology, particularly virtual reality. Rosen received his B.A. in biology from Cornell University in 1974 and his M.D. degree from Stanford University School of Medicine in 1978. Rosen has helped develop a computer-based and scenario-based training system for combat casualty care for the Advanced Research Projects Agency (ARPA) and has written white papers for the Navy outlining recommendations for education and training related to virtual reality in medicine and military operations. He was a senior fellow to the C. Everett Koop Institute at Dartmouth from 1997-1998, where he worked on development of a telemedicine system for the Lakes Regional Area in New Hampshire. He served on an Academy of Sciences committee on the role of Virtual Reality Technology that published its report in 1995, and on a National Research Council committee for the Navy on Emerging Technology Threats 2000-2035 that published its report in 1997. He was also on an advisory panel for NASA in 1999 on Medical Care for the Mission to Mars in 2018.

Cybercare: Responding to a Mass Casualty Event in the 21st century

Joseph Rosen, MD

Abstract

In the next decade it is likely that we will be faced with a mass casualty event in the United States either from a natural disaster or a terrorist attack. For example our present healthcare system would be overwhelmed rapidly by a bio-attack using a weapon of mass destruction such as a bioengineered virus. The ideal U.S. healthcare response system would consist of, a national command network that would control a large set of resources. These resources would include telemedicine, telerobotics, health care first responders, and major medical centers all electronically linked together throughout the country.

This new "cybercare" healthcare system will be immediately available to respond to a large catastrophic event, in one or more localities, from distant multiple remote command and healthcare response teams. The system would be designed to handle the following scenario: the release of a ’new’ virus that would cause a catastrophic event in a major city and then spread in a ’dandelion’ fashion encompassing multiple new sites within a short time of onset. The cybercare healthcare response system will quickly assign distant healthcare sites to act as remote protected telemedicine response resources to respond to sites that have been attacked.

This new cybercare healthcare response system would combine a number of critical technologies. These would include both information technologies and physical technologies. Telemedicine, telesurgery, telemonitoring, virtual reality, augmented reality, telecommunications,and intelligent software agents would all make up key parts of this system. The system will utilize remote-controlled robotics in conjunction with responders at the incident sites, as well as autonomous robots. It would require a flexible command structure so that command can be shifted to any part of the network as the attack progresses. The cybercare response network will have to encompass most of the U.S. to have the necessary resources to respond to a large catastrophic event.

The recommendation of this report will be to develop a research agenda to create a system to response to a catastrophic terrorist attack that would normally overwhelm the present local, state and federal agencies, and interagency groups. In these extraordinary circumstances a special agency or system maybe required to respond and institute the recovery from the terrorist event. This system will require an integration of resources in a flexible matrix approach that can respond rapidly and dynamically to an attack on our nation (see Extreme Information Infrastructure).

What is this system?

The system will first need to be modeled and its components identified. These components will need to be developed on a expedited schedule, if they are not already developed, or are being developed by one of our agencies.

The system would then need to be developed in a large scale simulation environment - MEDNET (like SIMNET). Once established as a simulator it will need to be deployed as a 'performance machine' where each of its components are operated from distant remote protected sites, such as in a tele-operation model. The command sites will direct resources at the sites that have been attacked -these resources will include humans, tele-operated machines, and equipment and supplies.

In this way a national network of command resources will be immediately available to respond to a large catastrophic event in one or more localities or states from multiple remote command response teams. This catastrophic event(s) may then spread in a 'dandelion' fashion (as seen with small pox and cyber threats) encompassing rapidly multiple new sites which will be quickly assigned new distant command sites to respond to them. In some cases command sites will become infected and be switched to local response sites.

This system will require a level of tele-operations and augmented reality that has only in the past been used in isolated cases for specific operations like MOUT, underwater remote operations and rescue, response to nuclear contamination in nuclear power plant disasters, and most recently extensively in minimally invasive surgery throughout the country.

This system will also require a flexible command structure so that command can be shifted to any part of the network as the attack progresses. Overall command can be centralized, regionalized or remain de-centralized as best indicated.

The network will have to encompass most of the US to have the necessary resources to respond to a large catastrophic event, otherwise the network of response teams could in itself be overwhelmed as the number of local sites affected increases rapidly. (It could also employ response teams from international sites, NATO or other allies).

Each response site could be a remote command/response team assigned a specific task at the incident site or each response team can be virtual, made up of a number of individuals that have been previously trained together but now live at distant sites from each other. The team members will be networked together as they are brought online to work together and grouped according to their needed skills for this attack.

This system will need both remotely controlled operations (simple robots -MIT, UTAH, Stanford, JPL) for many tasks, some humans at the incident sites (with protective gear), and some autonomous robots for very simple tasks such as supply and logistics (See Carnegie Mellon autonomous robot program and Cybercare Robots).

The robots should not be seen as robots, but as their component parts -control/command units, sensors (vision and touch), motors and mobility, bandwidth and supportive structure. In some cases we shall only want to send in mobile-sensors, in other cases sensors with motors to perform a simple task like take a sample. In some cases enough band width will be available to remotely control these robots, in other cases they will need to be autonomous. IN some cases they will only need to transport supplied, in other cases they will need to establish basic utilities such as water, power and bandwidth.

The system and its network will be like the description of an army in Sun Tzu the Art of War - An army should be like a snake - if you attack its head it will response with its tail, if you attack its tail it will respond with its head, and if you attack its middle it will attack with both its head and its tail. All of the parts of this system have to have this flexibility. A multi-site, sustained attack is a very likely scenario in the future. It is one that we are least prepared for on our own domestic soil.

The component parts will need to be set in place like the Eisenhower defense highway system. This approach was a radical approach away from the hub systems of the railroads. The network envisioned will need the bandwidth of the internet that is presently laid down all over America like the Eisenhower system of highways. Or in the event of an attack large amounts of bandwidth will need to be laid down rapidly - which is true of any battlefield of the future.

With respect to the robots or their sub-components they will need to be assembled from multiple local depots where they are stockpiled. They should be reconfigurable according to the needs of the situations. They should be whenever possible remotely controlled. (They could be stockpiled in national guard armories, or at local police, fire department, or EMS departments). In some cases robots that are used for domestic production or services could be re-assigned, just as we use humans in dual purpose roles. (In the distant future the robots could be created as a generic workforce and then reconfigured as needed in the event of an attack. In an alternative approach they could be made up of many smaller components and could self-assemble and re-configure as needed).

As we move further into the future the technologies of robotics, genetic engineering, and nanotechnolgies will provide improved, miniaturized, flexible tools to support the above system (they will also play a significant role in the weapons). It is hoped that all of this will be realized by the year 2025. However, inspite of the critics who say you can not build this system now - all of the components of this system are presently available in small numbers. Many of the tele-operation systems have been available since the 1950's. The robotic systems have seen great advances in the last several decades. The types of simulators and virtual reality systems needed have been developed from the 1970's to the 1990's and used successfully in the preparation and training for the Gulf War (SIMNET and DMSO).

To put this 'system' together would require an effort proportionally or greater than the Manhattan Project. But just as in the Manhattan Project - the nation and our society was at serious risk. A catastrophic terrorist attack with a weapon of mass destruction whether it be a bioweapon or a cyberweapon, or a combination of the two could result in our society and its fundamental values being seriously compromised.

The time to develop a response and therefore a true deterrent is now. A system as we have presented would contain the threat before it spreads throughout a region and possibly the nation. It allows us to face in a very real way the enormity of a successful deployment of a WMD on our populace. But this system also gives us a response and method of recovery to sustain our national infrastructure and societal values in the face of such a threat. It is no longer possible to assume these threats will not happen. In the words of the secretary of defense one year ago "It is not hyperbole. IT is reality". It is only a question of time before we are faced with extraordinary challenges

National Institute for Urban Search and Rescue Requirements Committee

Bobby Hartway, Chairman

Charter: Develop the XII Blueprint

Members:
Brian Morgan
Robert Chartrand
Jeff Ribel

The committee emphasis over the last few months has been to produce an XII Blueprint Development Plan for the development and publication of the XII BLUEPRINT for Domestic Preparedness against Weapons of Mass Destruction and Emerging Infectious Diseases. The XII Blueprint will be a systems requirements document useful across all disciplines and at all levels of Government, Non-Government, Industry, and Academia during efforts to develop and operationally integrate the combined systems comprising Domestic Preparedness. The Blueprint will be based upon a total integrated systems engineering model of the Domestic Preparedness System. The committee is presently defining a systems engineering methodology that will be used to construct the integrated model. An early draft version of the systems model has been established and is briefly introduced here, but much work remains to be done. NSF grant funding is being sought to support a fulltime effort to finish the system model and then use it to develop and publish the complete XII Blueprint document.

This report describes the activities to plan the technical accomplishment of the XII Blueprint.

Efforts to acquire funding to 1) fully develop and publish the XII Blueprint and 2) use the Blueprint to develop and build the XII Development Testbed are described in the NIUSR Grants and Contracts Committee report.

Efforts to prototype and publicly demonstrate the enabling technologies available to implement an XII are described in the Technical Committee report.

This report follows a six step sequence as shown by the flowchart below.

[Figure: SEE ATTACHED FILE]

(1) What is The Domestic Preparedness System?

The purpose of constructing an overall model for the "Domestic Preparedness System" is to establish a common system environment model because it helps establish the present and future boundaries of the system. It doesn t matter whether these boundaries are firm or fuzzy. What is most important is to show what could be involved in the overall model, whether now or two decades in the future. The idea is to provide a basis for the big picture over the long haul. This big picture can then be subdivided and annotated as to what is real and right now, and what is fuzzy and somewhere in the future. The single most important purpose is to have an integrated whole picture that shows what the system is and could be to support collaborative discussion and integrated planning .

Our conceptual system model shows that the Domestic Preparedness system is truly a system of systems, many of which are not yet well defined, but which must one day be accounted for. What is most clear is that there are so many different organizations and disciplines involved, and so many different missions. Many of these entities respond differently to the same common "threat", and some entities have a unique threat. The important concept is that in the event of an "extreme crisis", many of these entities will have to work together as a single integrated operational system. Worse yet, each type of "extreme event" will likely require a different combination of entities to properly respond. In other words, the Domestic Preparedness System is a system of systems that will individually be required to very rapidly harmonize, synchronize and interoperate under unpredictable extreme situations. Sounds like the military concept for global joint rapid response force doesn t it? Sounds a lot like an oxymoron since joint and rapid are mutually contradictory. This is precisely why we call the solution an "extreme information infrastructure". Simply put, the system must have the flexibility that while each system is optimized for their specific and individual missions, they may be operationally and informationally reconfigured very rapidly so that any authorized operational entity at any location can have access to the right information at the right time. It is clear that at the present time, most of the entities of the "system" are not technically structured or jurisdictionally chartered to operate effectively outside their traditionally defined mission area.

[Figure: SEE ATTACHED FILE]

(2) Why are Requirements Needed?

The large Federal budgets established to address the problems associated with the threats of Domestic Terrorism and Emerging Infectious Diseases were created in an attempt to quickly implement programs to counter and diminish these threats. These funds were released in advance of any requirements other than vague references to the ominous dangers presented by the collective threats. The legislation authorizing the funding left it up to committees, working groups, and individual government departments and agencies to determine how best to allocate the funding. The GAO has issued several reports on the lack of sufficient overall coordination and the complete lack of requirements. The only mechanism to date set up by the Federal Government to establish an integrated set of requirements is several multi-agency committees and working groups. There is inadequate central authority to manage the committee and working group activities to any common goal. This means the implementation process for a Domestic Preparedness System is "Here is Money, Bring Solutions". Presumably, after enough of this process takes place, the resulting individual solutions can somehow be integrated into a cohesive, operationally integrated system. This has never worked in the past, and isn t likely to work this time. What will have to be done is to work out the integrated system requirements in parallel with the multiple implementation activities now going on, in the hope that when a system vision is finally acquired, the aggregated solutions can somehow be fused into an operational whole. This simply means a lot of retrofitting. But this will not be successful without a master integrated operational plan. It is difficult to imagine how a single integrated operational picture could be established without a total system requirements definition. It is difficult to see how a total integrated system requirements definition could be established without a total integrated system model. It is inconceivable how a total integrated system model could be established without using a systems engineering process. It is unlikely that an objective total view systems engineering process could come from some jurisdictional player from "inside" the system. It is therefore easy to see the very important role for the non-profit, multi-jurisdictional body of the NIUSR membership. This is the exact purpose for the NIUSR Requirements committee effort to develop a plan to produce the missing and critically needed systems model and XII Blueprint for the Domestic Preparedness System.

[Figure: SEE ATTACHED FILE]

(3) What is a Systems Engineering Methodology?

A systems engineering methodology is nothing more than a process that breaks a large complex system into enough smaller pieces that the system components and their individual interactions can be sufficiently defined to provide a single integrated operational model of the system.

[Figure: SEE ATTACHED FILE]

The process can be described as one of developing and defining all the different viewpoints one can take in looking at a system and its operations. For example top-down versus bottom-up. Every system has hierarchical levels, breadth and depth. Every system has distinct operations types and operational phases. By defining the various dimensions of a system, it is easier to focus any given discussion on characteristics of a model because there are now common viewpoints that can be shared.

The best way to visualize the system dimensions is to think of them as VIEWPOINTS of an exercise game participant. The viewpoints vary depending upon the hierarchical system LEVELs; (1)at the top are strategic policy, strategic planning, strategic operations C2, (2) in the middle are tactical planning, tactical operations C2, tactical logistics/dispatch, and (3)at the bottom are field operations C2 or incident command, and field response actions.
Coordination, interoperable communications, security/authority verification, and decision-support information are needed at every one of these levels, but they each look a little different at each level.

These of course are exactly the same levels we have always had in military systems. Professionals in the C4I business already know that there are tight parallels between military C4I and emergency management C4I. But one VERY important difference in emergency management that NIUSR adds is that COORDINATION adds a fifth C to make emergency management a C5I. This is because in combined operations in military systems, you have a rigid hierarchy of authority, whereas in emergency management combined operations you have a lot of "organizational anarchy" that requires coordination. So C5I is used to clarify the distinction between the usual military view and the emergency management view. On top of the difficulty of organizational anarchy coordination, you add the requirement for INTEROPERABILITY of multi-jurisdictional communications needed to make this already difficult coordination possible. Again, this is more difficult than combined operations interoperabilty in the military, because in C5I you are dealing with multi-jurisdictional, anarchical organizations.

Now, you add on the terrible condition that, oh, by the way, you will lose most of your normal communication links and networks during the disaster, so you will have to have backups. So you must make sure your C5I communications must be accessible and reliable during the disaster.

Finally, you add on security and authority certification across all levels and all jurisdictions in your organizational anarchy. And now you have the basic requirements for a C5I extreme information infrastructure (XII) system!

[Figure: SEE ATTACHED FILE]

But don't stop here. Add a new level to the hierarchy of levels from top to bottom. Add a level below the bottom C5I (tactical field operations) level. This new bottom level is the population or public level. If the C5I system is the management system, the public is what's being managed. The public includes the victims, worried well, bystanders, and public at large, as well as the media folks everywhere and in everyone's face. We call this viewpoint "inside-out vs. outside-in". Inside-out is the view of C5I towards the situation and the victims, public, media. Outside-in is the view of the victims, public, and media towards C5I. This may sound trivial, but you will be surprised how it, in addition to the other levels/views, helps divide the Essential Elements of Information into more logical groupings. So, there you pretty much have how to use a systems approach to visualize disaster/emergency management as a "system", and how to break up the requirements into different segments or pieces or viewpoints, in order to tackle them one at a time and keep them organized.

The final trick is to realize that this "system" looks different FOR EACH TYPE of disaster. It especially looks different for scenarios requiring extensive medical facility use and medical care providers and specialized medicines, as you have for bioterrorist events. Then, when you add in a contagious bioagent, it goes beyond our present ability to control. But there is hope through modeling, planning, exercise, and coordination.

There are ENORMOUS differences in how you handle the scenario management depending upon the type of threat agent. Contagious scenarios create very stressing time-factors and containment-control factors. You can liken this to stopping a nuclear chain reaction and trying to contain the radiation. If you don't do the right thing very quickly and correctly, it's all over, and irreversable. This is exactly why a plague or smallpox type scenario stresses any emergency management system. But staying with the analogy, a nuclear reactor doesn't stress out professionals in the nuclear energy business because they have completely modeled it, know exactly how to manage it, and have a lot of continuous practice. (Of course, accidents can still happen, but they try to model and practice those too!).

It will thus be helpful to define an intensity scale to the scenarios. You can define a continuum or scale to the level of scenarios, something like a knob or rheostat you could use to turn up "scenario HEAT". Everyday 911 type emergencies at the lowest setting, then on to large scale natural disasters (like FEMA does all the time) about a third up, to terrorist events using chemical agents (like sarin) higher yet, to terrorist events using bio-agents like Anthrax (infectious) even higher yet (maybe two-thirds), and then to extreme terrorist events like Plague (highly contagious) very high up (maybe nine-tenths), and finally, over the top (100+) would be combined extreme events, such as warfare-type combined chem-bio events (yes, some are talking about this) or a really really nasty natural bug like we had in the 1918 flu pandemic.

What is very interesting about this knob, is that you invoke different TYPES of response as you turn it up. For example, just because you can handle a very large natural disaster (FEMA type) doesn't mean you can handle even a small chemical terrorist event - - because you cross the boundary of the TYPE of response required! Most obvious is that Firemen, Policemen, HAZ-MAT, and EMS techs are not going to be the medical responders for biological disease agents, but they all DO need to be protected for their OWN safety against such agents.

When you train these first responders how to protect themselves and coordinate on-scene responses, you have only addressed one-half of the equation. The other half, which is causing all the recent exercise failures, is when you bring in the part about medical care facilities where all these victims end up. They are simply unprepared and haven't been much involved so far in the big "WMD" movement. Most exercises can't bring in the public health and medical care facilities as players simply because there usually is no way to "network" with them! Most state and local public health systems don't have much networking at all (some small local ones don't even have web access). Most hospitals, clinics, and other care providers each do their own thing. TOPOFF 2000 in Denver proved this out as being a real big problem area, but everyone is having a lot of trouble figuring out how you fix the problem, because there is no one in charge of the loose collection of health and medical care jurisdictions and institutions. The Public Health Service community is only just now getting slightly increased funding, and help from CDC, but the have a long ways to go. Each local area medical care faciltiy is necessarily motivated by the bottom line more than the common cause (unless someone pays them).

The point is that if you turn the scenario knob up just one little notch past chemical terrorism, you go into a whole new world or required response types. A small area Anthrax attack turns the knob just a crack into this new area, and a larger wide-scale anthrax attack immediately takes you into another dimension of response altogether, namely the medical facilities and health care side. When you add contagious bio-agents (natural or terrorist), the response requirements go critical.

There you have it. The basic components of a systems approach for modeling the Domestic Preparedness System. You have the scenario rheostat, the system levels, the system views, the coordination, the communications, the security/authority certification, and finally all of these versus different types of disaster scenarios.

(4) What is a Total Integrated Systems Engineering Model ?

A total integrated system model is the descriptive system model resulting from using the system engineering methodology and viewpoints described above. The advantage of a single integrated system model is that the individual components may then be worked in parallel, in any order, with assurance they will correctly interface as a single cohesive whole when put back together. This is obviously exactly what is needed for the Domestic Preparedness System. The trick of course is to first have a good description of what the system is. In absence of this, and if starting with an existing system or aggregate pieces that are to be made a system, the system must be synthesized from information gained by reverse engineering. This can be done by aggregating the existing parts, looking at their individual requirements, determining their interfaces, and then reverse engineering any translators as needed to make them mutually interoperable. This is exactly the situation with the Domestic Preparedness System. The individual component parts are individually known, but not described anywhere in sufficient detail that a composite picture may be painted. The trick here is to construct a generic system model that allows placeholders for all the existing pieces to plug in when information is gained on each. When sufficient information on all the pieces is acquired, the multiple interfaces may be investigated and specified. Translators, retrofits, or re-engineering efforts may then be identified and undertaken.

The draft concept for the NIUSR System Model for the U.S. Domestic Preparedness System shows the basic structure for beginning the system modeling process just described. You can see it has most of the basic dimensions discussed above in the systems engineering approach. There are many many details to be added for each of the simple components shown, but the basic structure is there to support collaborative discussion. Closer inspection will reveal that this model shows system features from only a single jurisdictional viewpoint. A "depth" must be added to each entity to account for the jurisdictional divisions of Government, Non-Government, Private, and Industry.

You must also realize that every single arrow in the system model diagram indicates an information interface. Each of these interfaces implies a network connection, a message protocol, a data format, and of course a scenario context for when each type of data should be available or broadcast, and who is authorized to handle that information.

(5) How will the XII Blueprint be produced?

The Requirements Committee blueprint development process is a bottom-up process. It starts with taking a fresh modeling look at the entire integrated system concept of crisis and consequence management for the Domestic Preparedness System. It will go further than most other models by considering interfaces with the total Health Care System from top to bottom in addition to the usual "WMD" entities and interfaces. In addition to better supporting bioterrorism scenarios, this newer part of the model will address the recent concern for Emerging Infectious Diseases (EID). This new part of the model is crucial to Bioterrorism scenarios, which become delayed response medical problems. The model also considers interfaces with the Global Disaster Information Network (GDIN) program, and DoD s renewed interests in Operations Other Than War (OOTW) programs. The product resulting from employing this bottom-up process will be a documented system architecture description, the XII Blueprint. Preliminary work on this document serves as a base reference for NIUSR projects for any specifically targeted funding area.

[Figure: SEE ATTACHED FILE]

(6) Exactly what is the XII Blueprint?

The XII Blueprint comprises the technical and operational requirements for an evolving and totally integrated XII System that will fully support the Domestic Preparedness System. It defines XII functional system components and their operational and technical interfaces at each operational level in the system and for each operational phase of an extreme event. The Blueprint will serve as a "living documentation" of evolving XII System Description and System Requirements. It will be a funded extension of work now being done in the XII Requirements Committee by volunteers.

The XII Blueprint will be the system requirements for the NIUSR project to implement the XII Development Testbed. The XII Development Testbed will be a stand-alone installation of an operational software suite and equipment set comprising an XII development system in some customer/sponsor specified location. This equipment set will not have to be tied to any specific facility — it would in fact be "transportable". The equipment set development will be a funded extension of the volunteer work now being done to produce the periodic XII Games

Demonstrations, such as the present "When Disaster Strikes" tabletop game and workshop being held here now in Las Vegas. The basic testbed would be software configurable to function as an operational center model for any jurisdictional entity at any level in the Domestic Preparedness System.

Conclusion

1) A plan has been established that will provide a structure to produce the XII BLUE PRINT.

2) The initial development of a Domestic Preparedness System Model has begun. It is being used as the basis to develop the Implementation Plans for the XII BLUEPRINT document and the XII DEVELOPMENT TESTBED.

3) We hope to be able to make available through the NIUSR website the draft material of both the Domestic Preparedness System Model and the Systems Engineering approach used to develop it. The free availability of this material should encourage better participation and collaboration among NIUSR membership by serving as a common roadmap or point of reference. (Remember that NIUSR membership is a multi-disciplined, multi-jurisdictional group representing all sides of Domestic Preparedness —Government, Non-Government, Industry, and Academia.)

4) This draft material will be useful to the Grants and Contracts Committee in support of the effort to capture funding for full development of the XII BLUEPRINT document and the XII DEVELOPMENT TESTBED.

5) We need more membership participation in this critical activity, and anyone interested is encouraged to join the effort.

Cybercare Robots

Neil J. Fisher NREMT

Summary

Currently there isn t an effective, safe way to handle this form of Bio-HAZMAT threat. Current methods involve setting Control Zones , and specially trained teams in NBC suits. The response times are relatively long and the risk to the team is high. Local Emergency Management teams are ill equipped to handle these circumstances. First Responders would quickly succumb to the virulent disease.

Technology exists now that would significantly reduce the death toll among citizenry and emergency response personnel. All Terrain Robots, with GPS and autonomous behavior systems could be used to distribute vaccine, official information, monitor the situation at multiple sites, and provide a direct link to local and remote response personnel.

Problem

In mass casualty situations, where the standard infrastructure breaks down, new infrastructure must be brought in to replace the missing pieces. Injured civilians, first responders and other medical personnel will require treatment. Relief and decontamination efforts will be daunting, and as time goes by will become increasingly more difficult to manage. At the present time specialists and special equipment have to be brought in from around the country. This process is extraordinarily dangerous, takes time, and is expensive.

Terrorist situations that invoke Presidential Decision Directive (PDD-39) and the Federal Response Plan (FRP) terrorist and chemical and biological Weapons of Mass Destruction (WMD) annex, are essentially "worst case scenarios". In these situations, as in the fictitious news report above, FEMA, the FBI, the National Guard, along with local Emergency Management personnel, are faced with a complete (or near complete) breakdown of local infrastructure. Other problems that must be dealt with include the physical and emotional state of symptomatic and non-symptomatic persons in the hot zone.

Solution

iRobot Corporation has demonstrated autonomous GPS waypoint following, and swarm coordination software in various public demonstrations. This picture is a composite photo of the test track at Montgomery County Fire Rescue Training Facility, in Rockville, MD using data from a test run this September. GPS waypoints were entered into an Operator Control Unit through a graphical interface similar to the satellite image shown here. An Urban Robot equipped with a differential GPS receiver followed a randomly selected path so accurately that the deviation cannot be seen at this scale. This software was developed as part of DARPA s Tactical Mobile Robot (TMR) program.

Figure: See Attached File

Robots could be used in this type of mass casualty scenario in a variety of ways. Large all-terrain robots similar to iRobot s ATRV could be strategically located throughout a city, or in close proximity. These robots would be deployed in time of crisis to deliver medication, and provide a communication link to field command, or relay to a remote command center. Loud speakers mounted on the robot could deliver official information, while onboard cameras, microphones and other sensors monitor activity near the robot.

Figure: See Attached File

All of the necessary technology for such a robot exists today. An ATRV has been modified to carry a medical payload (vaccine for instance), and be equipped with the GPS waypoint following software, and satellite tracking. Multiple robots could be controlled by swarm behavior models. The advantages of using an ATRV type platform are: Simplicity, high maneuverability, rugged, low cost, proven technology, reliability, and simple maintenance. Presently ATRVs have approximately a ten-mile range. They are equipped with cameras, sonar sensors. Laser scanners, onboard computers for obstacle detection and avoidance, and vision processing systems. The addition of attitude and inertial guidance packages would complete the sensor suite. With simple routine maintenance, an ATRV could stand ready for several years.

In the near future, with sufficient funding, a number of technological enhancements could be made: battery and computer technology will continue to improve; autonomous behaviors will continue to be developed; running times will be extended; on-board processing capabilities will be increased. Robot capabilities increase exponentially. These trends will continue over both mid-term (five year) and long term (ten plus years). Sensor and communications technology improvements coupled with advances in software, will allow the robots greater situational awareness and flexibility in obstacle avoidance. Cooperative behaviors between robots will enhance the capabilities of the robotic team. Included with the collaborative ability of the team would be real-time dynamic mapping of the contaminated area including biohazard and casualty data, giving the Incident Commander the ability to always work from the most up-to-date information. Based on the latest information the Incident Commander could alter individual unit objectives to better achieve overall mission directives, or if necessary, redirect the entire team. The enhanced communication ability of the team will allow temporary a communication infrastructure to be set up quickly and efficiently. Robot survivability will also be an issue. Not only will the CybeResponder need to be able to withstand the rigors of the environment, it might have to survive mobs of panicked people. The best solution to this dilemma is to use simple robust technology.

Five Years from now, the robotic team itself would have the ability to find alternate routes, and modify individual goals, to achieve the overall mission objective. ODOA and sensory situational awareness will advance to a state where dynamic obstacle detection, trajectory and path planning will be robust and reliable enough to avoid moving traffic on busy streets. Other behaviors that would be implemented in the five year time frame might be crowd response behaviors, use of visual information to identify humans, anti-handling/anti-tampering, and self-righting.

Possible crowd responses would be based on observed crowd behavior. Someone might try to damage the robot if it were perceived that the CybeResponder is not distributing vaccine fast enough. The robot might respond with a series of warnings followed by a non-lethal defensive maneuver, such as directed pepper spray, or possibly electrically charging the outer shell of the robot. Self-righting may also be useful here, in addition to inversion due to unexpected obstacles or unstable terrain. Visual identification of individual persons can be helpful in the distribution of vaccine, either in denying medicine to those who have already received some or in seeking out those who have not or are unable to seek help on their own.

Ten years in the future, the possibilities and potential of robotic first responders will begin to approach the abilities of human first responders, and in certain areas surpass them. Advances in material science will allow lighter, more powerful and more maneuverable mechanical chassis. Mechanical, electrical and software systems will be tightly and seamlessly integrated. Thus resulting in unprecedented durability and reliability. Robot responders will be able to perform complex self-diagnosis and limited self-repair. Further advances in cooperative behaviors, and specialized robotic team members will expand the role of the Robotic Response Team. Economic pressures will continue to drive down the cost of technology, enabling local staging of response teams in all major metropolitan areas. With increased capabilities will come increased usefulness and greater deployment possibilities. Robots serve as first responders for all HAZMAT and Mass Casualty events. Robots could serve as Paramedic and HAZMAT Technician Assistants, Robotic Responders could spend extended periods of time in the "hot zone". Greater emphasis on autonomy, with voice recognition software would allow the Cyber Responder to converse with victims, and report findings to incident command.

Relevant Technology

iRobot Corp manufactures many types of outdoor all terrain robots.

Urban Robot

The Urban Robot“ is an enabling technol-ogy that provides unprecedented mobility over terrain that previous robots could not negotiate. This self-righting, tracked robot can climb over urban and rural terrain includ-ing curbs, rubble, standard stairs, fields, and sand.

The Urban Robot was developed under con-tract with DARPA s Tactical Mobile Robotics (TMR) program whose goal is to develop autonomous vehicles for reconnaissance and surveillance applications. The first Urban Robots were built as research tools that are currently in use at Carnegie Mellon University, Georgia Tech, University of Southern California, SRI International, the University of Pennsylvania, and the Spe-cial Operations Forces of the US Military. The upgraded urban platform has been developed for commercial use and is being manufactured and sold by our RWI Divi-sion. Urban Upgrade Robots are now in use at a wide variety of sites including Jet Propulsion Labs, Oakridge National Labs, Honeywell and Southwest Research Insti-tute.

Figure: See Attached File

The urban robot measures approxi-mately .63 L x .50 W x .13 H meters. Its small size makes it diffi-cult to detect and offers a minimal shipboard footprint. During urban warfare testing at Ft. Sam Houston in October, 1999, the low profile made it difficult to target and disable through gunfire.

The system was designed to with-stand repeated impacts experienced in typical operations. Testing at Ft. Sam Houston showed it to survive repeated hand tosses over a 2 meter high fence onto earthen landing zones. This allows the possibility for the robot to be deployed in MCM operations from other delivery vehicles including a low altitude helicopter.

Operation is simple and achieved by a single hand-held computer mouse-like input device. Situational awareness data (camera, position, sensors) is displayed to the operator and can be recorded for future analysis. The robot is based on a computer brain which controls the communications, motors and various sensors. This facili-tates the addition of customer add-ons such as special cameras, mine detection sen-sors, thermal sensors, GPS, etc. This digital control architecture offers easy integration and compatibility with existing Command and Control Systems. Payload capacity is approximately 20 kg and battery operation time is approximately 2 hours.

We are currently developing the next generation of this robot. Advancements for this platform will include waterproofing, mechanical manipulation, autonomous behav-iors, modular payload and sensor addition, faster speed, longer battery run time and lower production cost. This robot will be available for demonstration in September 2000.

K8 Rapid Response Robot

The K8 Rapid Response Robot is designed as a tactical scout robot a rapid deployment tool to provide on the scene commanders with the critical, up- to-the-second audio and visual intelligence they need to make swift, defensible, informed decisions. K8 scouts the way for entry teams while serving as a potentially life-saving "trip wire" to determine a suspects state of mind, capabilities and intent. Because it is neither armed or armored, K8 is highly unlikely to be used by a suspect as either a weapon or shield.

Due to its small size and rugged construction, the K8 can be carried in standard patrol units right to where its needed where it can be quickly deployed to assist in the search for fleeing suspects, domestic disturbances, etc. without having to call out a dedicated unit. Wherever your team can go, the robot can go Including up stairs. With no bothersome tether to get tangled, the K8 can turn in the tightest hallways and doors.

Figure: See Attached File

Packbot

Packbot, the next generation of Urban Robot, takes the man-packable robot to the next level. It features quick-change batteries and fast release flippers. Packbot is a man-portable robotic platform with onboard computer processing.

The platform will be capable of speeds of up to 4 meters per second and run times of two or more hours. Packbot will be able to withstand shocks of up to 400 Gs and will be waterproof to 3 meters. Packbot will be a combat-ready system, and will posses many autonomous functions. Through the combination of autonomous and assisted tele-op behaviors, Packbot will be able to follow preprogrammed routes, circumnavigate obstacles, climb stairs, scout out new and alternate routes, and relay sensor data to a command post.

The Packbot is the centerpiece of the U.S. Government s Tactical Mobile Robots (TMR) program whose goal is to develop autono-mous vehicles for reconnaissance and surveillance applications. The goal of the TMR Program is to increase the information of hazardous threats while reducing the potential for harm to humans currently providing this function. PackBot is a tracked vehicle, similar to the Urban Robot, that incorporates forward-articulated tracks to aid in stair climbing, sensor positioning, self-righting, and high centering recovery. This vehicle is highly robust, easily man-portable, and has demonstrated extreme mobility in var-ied terrain.

In Phase I of the PackBot project, iRobot devel-oped a proof of concept tracked mobility plat-form that incorporated forward articulated tracks. Under Phase I, a complete system design was developed including the robot, a wearable user interface, and system programming. The sensor package, including vision for navigation and tracking, is tailored to the mobility system and integrated into the system architecture. The PackBot robot weighs approximately 18 kg and can be compactly stowed for easy transport without the need for special equipment.

The next design iteration was the PackBot/Urban II platform, which added environmental ruggedness. The latest iteration added new electronics featuring PC-based control.

During recent evaluation exercises with the U.S. Army Engineers at Fort Leonard Wood, MO, a single soldier easily carried the PackBot by backpack, allowing free use of both hands. The robot can be quickly and easily inserted into otherwise unattainable locations.

The PackBot offers an unprecedented level of mobility through varied terrain and rugged environments. The robot can readily right itself after tipping accidentally or on purpose by a disabling attempt by enemy forces. Using its forward tracked articu-lators, it can climb stairs, rocks, curbs, hills and ramps, and stand upright to navigate narrow twisting passageways. The robot can move on land at speeds up to 2 m/s.

The control system of PackBot will enable rapid response to environmental stimuli of its sensors, such as cameras, attitude sensors, sonar, thermal/infrared sensors, magnetometers and heading sensors, each specially tailored to the unique system architecture. Sensors customized to specific missions can easily be integrated into the system due to its modular architecture.

ATRV

The rugged, reliable ATRV is the mobile robot of choice for demanding all-terrain projects. Its low center of gravity, big knobby tires, large ground clearance, weather-resistant enclosure, over 220 pound payload capacity, plenty of sensor coverage and long run times enable the ATRV to overcome obstacles that would stop most any other robot. The ATRV was designed as an all purpose robotic platform. It s large size, multiple batteries, payload capacity and sensor coverage, make it an ideal choice for the CybeResponder.

The ATRV s hardware and software architecture is shared across the product line, allowing developments for one robot to be shared across all of iRobot s research platforms.

Figure: See Attached File

Mobility“ Software

The iRobot s Mobility robot integration software system represents a breakthrough in the design of software systems for robots and RCV’s. The vision of Mobility is to provide a means to rapidly develop interchangeable control software for a wide range of robot and RCV systems. The latest implementation of Mobility (the second major revision of the system) is making the vision of the reuse of interoperable soft-ware components for robot and RCV control a reality. Mobility is being used to build the software required by several commercial and DOD development projects on a daily basis.

Mobility includes a set of basic reconfigurable services for mobile robot and RCV hardware control, abstraction and management. We provide services for servo motion control, odometry, sensor processing, image capture, video compression, and many more. There are also graphical tools for connection and configuration of the software components. Parameters for each component can be adjusted and data-flows between components are graphically specified on-line, using these tools. The basic control mechanisms and sensory processing for some new robots can some-times be created entirely without programming, but through reuse of existing com-ponents and our component configuration management tools.

The Mobility system also supports a set of more advanced services that are used to provide robots and RCV’s with features like mapping, navigation and driver assist behaviors. These advanced services can greatly reduce the mental and physical load on the operator of the RCV by using information available to the robot to provide quick reactive responses to difficult situations, such as a collision avoidance or self-righting driver assist behaviors.

Mobility based software systems are built from collections of dynamically config-urable, pluggable software components. These components work together by con-forming to strictly defined interface definitions for every aspect of component functionality. Pluggable software components work together like your TV, VCR and wall outlets do; you connect compatible interfaces (power to power, video to video) and it works together. The connectors on your TV are also shaped so that you can’t plug video into the power outlet. Mobility provides this same kind of pluggable con-nectivity and error protection for software components by following the CORBA 2 standards defined by the Object Management Group (OMG). The OMG is an inter-national consortium of commercial software companies that work to define stan-dards for high level interoperability of software systems. Mobility specifies all internal and external system interfaces using an open specification language called Interface Definition Language (IDL) that is defined as part of the CORBA 2 specifi-cation.

Mobility follows applicable OMG defined Common Object Service (COS) inter-faces and defines new robot and RCV specific interface suites that are used to repre-sent, coordinate and control all of the elements of robot and RCV systems, as in the existing Urban Robot. These iRobot defined interfaces can be made openly available using the openly defined IDL format and others may write software that utilizes all the features of Mobility by following these interface definitions and the open com-munications standards defined by the OMG.

By combining open standards like CORBA with highly reusable and configurable robot component software designs, the Mobility robot software integration system helps iRobot deliver unprecedented robot capability and interoperable interfaces in one tightly integrated software system.

FARnet“

FARnet is a high speed, low and predictable latency, local area network architecture. FARnet is optimized for communication with and control of large numbers of heter-ogeneous sensors and actuators, in an environment where fast and real-time are both critical requirements. We anticipate that the use of FARnet will lead to significant advantages for Cyber Response Vehicles in weight reduction and modularity.

Deployer

The goal of iRobot s Deployer Project is to support small robots that DARPA has developed under the MTO Distributed Robotics program. We will develop a larger general-purpose robot to transport and deploy these smaller specialized robots to areas of interest. The larger robot will provide high-speed long-range transportation over various terrains to place the specialized small robots near where they can accomplish their tasks. After the smaller robots have succeeded at their tasks, the Deployer vehicle may collect and extract them.

The Deployer vehicle will also provide communications relay and power when necessary for the small robots. A critical part of this work involves coordinating the larger vehicle with the smaller vehicles and collat-ing the data from multiple small robots in the larger robot for transmission back to a base operator. The number of mission com-mands needed from the operator is being substantially reduced under our supervised autonomy control paradigm.

Swarm

The goal of the Swarm project at iRobot is to develop techniques for programming a distributed group of autonomous robots. Pro-grams for individual robots need to be robust in the face of complex environ-ments, and the group software needs to be tolerant to the failure of any number of individuals. The algorithms developed must be designed to be completely scalable, that is to function with groups of 10 or groups of 10,000.

Each individual robot is programmed using our proprietary Behavior Language software, running on top of our Swarm multi-robot operating system. This allows us to develop and test software at the individual and group level rapidly. A centralized data acquisition system for determining each robot s position and status in real time is also under development. This will allow us to define and measure global metrics to judge the success of our algorithms.

At the heart of the swarm project is the ISIS communication system. This propri-etary hardware lets robots communicate with their neighbors using infrared light. The system also allows a robot to determine the relative bearing, orientation, and range of all the robots it is in communication with. The communication network formed by these local interactions allows information to propagate throughout the entire group of robots.

The combination of local spatial relationships and group sharing of information gives the swarm powerful abilities. For example, the robots can position themselves into an arbitrary user defined shape, or the current physical arrangement can be uploaded to the user, forming a map of the explored area.

In addition to explicit communication with the ISIS system, individual robots will also be able to communicate with others by leaving trails in their environment.

The list of potential applications of this research is prodigious, including mine countermeasures, nuclear/biological/chemical threat detection, or covert surveillance.

Summary

The likelihood of Local, State and Federal Emergency Response Teams facing a catastrophic Biological Weapon incident is constantly increasing. Technology now exists that could greatly increase the survivability of both the general populous and of the Emergency Responders themselves. The technology developed by iRobot Corporation is scalable and provides a clear upgrade path for future platforms. Continual improvements in our technology, will expand the capabilities and roles of future CybeResponders. The autonomous abilities of CybeResponders will advance in step with developments in software and sensory technology. CybeResponders either alone or in teams will save lives, save time and save money. Robotic Response Teams will be ready and able to assist in HAZMAT mass casualty incidents, now, and into the future.

Information Technology and the Medical Response to Bioterrorism

Jon C. Bowersox, M.D., Ph.D.

Introduction

Medical preparedness will be a key factor in mitigating the damage caused by terrorist attacks. The United States has developed a well-organized emergency management system for responding to domestic catastrophes, primarily based on experience with natural disasters such as hurricanes and earthquakes. The existing disaster system will be applicable to attacks with conventional, nuclear or chemical weapons, where the peak incidence of injuries will occur at the time of attack. The Incident Command System developed and used by the Federal Emergency Management Agency (FEMA) is designed to enable a rapid response to a single sentinel event. Medical information management in these situations will be focused on command and control issues including patient retrieval, triage, and optimal utilization of limited clinical resources.

In contrast, the specter of bioterrorism poses management challenges more analogous to disease epidemics, in which the time from detection to eradication may span weeks. The onset of casualties will be insidious and difficult to recognize, the prevalence of disease will increase with time, and the affected population may be widely dispersed. The first responders to a bioterrorist attack will be primary care physicians, nurses, pharmacists, and hospital emergency departments, not paramedics and law enforcement personnel. Public health resources will be critical for epidemiologic investigations and infection control. Capabilities for remote evaluation and treatment must exist, particularly in the likelihood of community quarantine. A robust information technology system that will meet these needs, and be integrated with the medical command and control network must be developed (Table 1). Fortunately, the widespread proliferation of communication and computing capabilities throughout American society provides the opportunity to create a comprehensive information management strategy for combating bioterrorism.

- Surveillance and disease detection
- Pathogen identification (diagnosis)
- Prophylaxis and treatment
- Information dissemination (news, education, self care)
- Monitoring of response to treatment
- Coordination with disaster response command and control elements
- Forensic analysis (law enforcement)

Table 1. Health information technology needs for responding to bioterrorism.

Health Information Technology

Health care in the United States is a $1.1 trillion industry, employing more than 10 million people. Surprisingly, the use of computers in health care has lagged far behind other sectors of the economy. For example, transportation and financial services industries have invested 10-12% of annual revenues in information technology over the past decade, compared to only 2-5% in health care. There are several reasons why physicians and others have been slow to integrate computers into their practices. Health care remains a cottage industry, with more than half of the nation s 600,000 physicians in solo or small group practices. There are 5,000 hospitals and more than 3,000 health insurance companies in the United States, each with their own proprietary computer network. Standard data formats are only now starting to be widely implemented, and there is virtually no interoperability among health information systems from different vendors. Despite the economic clout of the health industry, physicians and hospitals operate on low profit margins, making significant capital investments in information technology difficult to justify.

Currently, computers are mainly used for administrative functions, including patient registration and accounting. Virtually all patient visits result in a claim form being submitted for reimbursement, or for resource tracking in the case of government or managed care organizations. More than one billion claims are submitted each year in the United States. A standardized diagnostic coding system is used nationwide (International Classification of Diseases, Ninth Revision, Clinical Modification, ICD-9-CM). Although only 50% of all claims are currently submitted electronically, by the year 2005 all claims will be processed through web-based systems, using standard (HL7) data formats. Other areas of increasing use of computers are for clinical record keeping and patient management. With the rapid growth of the Internet, consumer health informatics is emerging as a key area of future development (Table 2).

- Administrative (patient registration, eligibility determination, accounting, lab reporting)
- Clinical Record Keeping (laboratory results reporting, electronic medical records)
- Patient Management (telemedicine, digital radiography)
- Consumer Health Informatics (info portals, education, disease management)

Table 2. Applications of information technology in health care.

The pharmaceutical industry has been more effective in using information technology for handling prescriptions, with electronic data interchange enabling rapid authorization and claims processing by most insurance companies. Furthermore, automated inventory management is used for tracking prescribing patterns, and for just-in-time ordering and supply of over-the-counter and prescription drugs. Pharmaceutical companies gain access to a wealth of information that can be used for targeted marketing to individual physicians and consumers.

Information systems are widely used in clinical laboratory management and results reporting, however, it has only been in the past few years that standardized formats for handling health data have been developed. Health Level 7 (HL7), a messaging format used by 97% of large hospitals and 80% of all health organizations, has been adopted by the Centers for Disease Control and Prevention (CDC), commercial laboratories, and state health departments as the standard for the electronic transfer of laboratory data. Although enabling automatic transmission of microbiology results across systems and interfaces, state and local health departments have not agreed upon a common set of data required for disease reporting, which has limited implementation. When these issues are resolved, rapid reporting will greatly enhance disease surveillance and epidemiologic investigations.

Clinical care is still based on direct contact between patients and their physicians. Telemedicine has been available for more than two decades, but is used by less than 1% of all health care providers on a regular basis. Hardware costs and telecommunication charges have been prohibitively expensive until recently, and only government-subsidized programs have had sustained use. Liability and lack of reimbursement for teleconsultations have also hindered adoption. Institutions that have had the greatest success with telemedicine are those providing specialty expertise to rural areas and prison populations, where distance and security risks tip the cost-effectiveness balance toward remote care. As the reach of broadband telecommunications networks (e.g., DSL, cable modem) extends into homes and small medical offices, the use of telemedicine will likely increase. Telemedicine will have its greatest value in providing specialist expertise to smaller communities, and for extending care to remote or hazardous environments.

The rapid growth of the Internet, and the availability of cheap and powerful computers with online connectivity will dramatically change the practice of medicine over the next decade. In 1996, only 20% of physicians had computers in their offices; in 2000 almost 90% of medical offices are online. Consumers are frequently using the Web to access health information and services. Of the 116 million Americans who access the Internet, 70 million visited health-related sites last year. Web-based programming using emerging standards such as XML and Java, may also stimulate the development and eventual implementation of electronic medical record systems.

Portable, wireless computing is on the horizon. A consortium of cellular phone manufacturers has developed the Wireless Application Protocol (WAP) that will enable cellular phones to become Internet portals with web accessibility. Portable computing devices (PDAs) will also become mobile workstations as products incorporating Bluetooth, an international specification for broadband wireless interconnectivity, become available. Handheld, mobile devices will be used for remote physiological monitoring, point-of-care laboratory testing, clinical record keeping, and telemedicine. Voice recognition technology will be incorporated into these devices, eliminating the need for writing or keyboard entry.

Televisions and telephones, present in more than 98% of U.S. households, are frequently used as sources of health information. Cable and broadcast networks have an ever-increasing selection of health-related programming, primarily focused on entertainment. The Public Broadcasting System is a potential venue for consumer education about health issues. Telephones are ubiquitous, inexpensive, and highly effective as an interactive medium. A number of managed care organizations are using telephones for nurse-based triage and algorithm-driven care. The use of telephone-based, remote monitoring is increasing, particularly for managing chronic diseases and for cardiac telemetry. Thin-client computing devices use televisions as display monitors, and can connect to the internet through cable or dial-up modems, providing networked computing through common, and familiar appliances (e.g., WebTV).

Public Health Informatics

The CDC has been spearheading efforts to develop electronic tools for national disease surveillance and enhanced preparedness among state and local public health officials (Table 3). The Health Alert Network (HAN) is an internet-based system that will link local health officials into an integrated, nationwide system for epidemiologic investigation, training, and rapid communication. The National Electronic Disease Surveillance System (NEDSS) is being developed to integrate the many disease surveillance systems currently being used, incorporating tools for interpretation, analysis, and reporting of data through secure networks. Standards for those data elements required for electronic laboratory reporting are being established through the Common Interface for Public Health Electronic Reporting (CIPHER). Epi Info 2000 is a Windows-based software application for use by public health officials in conducting outbreak investigations, and for managing public health databases. CDC also sponsors BTTv, an educational tool using live and archived video streaming for bioterrorism preparedness and response. Although currently focused on educating public health practitioners and officials, educational modules can be readily customized for all levels of health care providers, and for the public. The World Health Organization is developing internet- based software for global epidemiology and identification of emerging diseases,

- Health Alert Network (HAN)
- National Electronic Disease Surveillance System (NEDSS)
- Common Information for Public Health Electronic Reporting (CIPHER)
- Epi Info 2000
- BTtv

Table 3. Centers for Disease Control and Prevention (CDC) public health information technology initiatives.

as are a number of non-governmental organizations and universities worldwide. Currently, the CDC s efforts are focused on upgrading the capabilities of state and local health departments. The challenge for public health informatics developers will be in extending the reach of data acquisition and knowledge dissemination to every health care provider, and in automating the surveillance process.

Applying Information Technologies in the Response to Bioterrorism

Scenario-based planning is an effective tool for assessing risks, planning resource allocation, and training responders. A hypothetical, but realistic, bioterrorist attack will involve the covert release of a particulate infective agent into a public gathering. Within 48 hours, those exposed will develop respiratory symptoms. Some will purchase over-the-counter remedies from pharmacies and supermarkets. Others will call managed care triage nurses, or visit their primary care providers. The youngest and oldest, with the least pulmonary reserve, will be seen in hospital emergency departments. Gradually, culture specimens will be obtained and processed by local laboratories. Eventually, local and state health departments will become aware of an increased incidence of respiratory infections, and may initiate epidemiologic investigations. People will be aware that many of their neighbors and co-workers have become sick, and apprehension bordering on panic will ensue. By the time laboratory identification of a bioterrorist agent is obtained, and treatment recommendations are made, business and government productivity will have ceased, and it will be too late to implement effective disease prophylaxis and treatment. Chaos will spread to other communities in the country, and even around the world, as the fear of multiple attacks ensues. Over time, the incidence of new cases will drop, and the disease will disappear, but catastrophic damage to individuals and society will have been done.

Using the example presented, it is evident a well-developed health information infrastructure would enable an earlier, and more effective response to the crisis (Figure 1). An automated surveillance and detection system, based on a simulation and modeling network, would constantly monitor such data as ICD-9 codes from insurance claims forms submitted daily by health care providers. Constant monitoring of drug prescription orders and sales register data for over-the-counter cold remedies would be analyzed against epidemiologic models, with a geographic information system (GIS) overlay.

Automating data acquisition and analysis will increase detection sensitivity, and reduce the current dependence on human-based reporting and epidemiologic investigation. Precedence exists in systems that monitor telecommunications and Internet traffic for data elements concerning national security. When a detection threshold is exceeded, immediate review by an epidemiologic investigation service crisis team would occur, and if necessary the FBI and FEMA would be notified. An automated surveillance system would also contribute to forensic analysis necessary in determining attribution. Concerns regarding privacy and data security are important, but can likely be addressed within the context of the Health Insurance Portability and Accountability Act of 1996(HIPAA). HIPAA will require all users of health care information to meet stringent standards for ensuring patient confidentiality.

Figure: See Attached File

*Figure 1. Future implementation of health information technologies **(+IT)** in response to a bioterrorist attack will enable earlier detection, and will result in fewer total casualties compared to capabilities available today **(-IT)**.*

By enabling earlier detection, supplies for prophylaxis and treatment can be deployed more rapidly to the appropriately targeted population. Early involvement of media resources will lessen the apprehension and panic that will ensue. Content can be originated from a central location, but delivered locally. Although television, radio, and telephone will remain the primary modalities for information dissemination, the web will be a powerful tool for education, and for interactive assessment of psychological stress levels. Mental health resources can be mobilized from a national cadre of trained responders, who will be able to perform counseling using web-based, interactive video. The interactivity provided by video conferencing will also be a powerful tool for satisfying human needs for social intercourse if quarantine conditions are imposed.

The other application of telemedicine will be in rapidly establishing the virtual presence of physicians and other specialists who have a recognized expertise in biological warfare, and who have trained together as a team. Peer-to-peer communication with community health personnel will facilitate mentoring as the medical response evolves, and will enable medical leadership to be maintained at the local level.

Monitoring the response to treatment will be greatly facilitated by electronic medical records systems. Using HL7 and XML standards, data elements can be readily abstracted for tracking appropriate physiological parameters, such as temperature and respiration, and laboratory results. The next generation of medical devices, including ventilators and intravenous infusion pumps, will incorporate Internet chips, with a unique IP address, enabling remote adjustment of parameters. The additional functionality provided will enable the delivery of care in hazardous environments with less risk to local personnel. Also, therapy could be provided in a patient s home or shelter if hospital resources are overwhelmed.

Although information technologies have tremendous potential benefits in improving the medical preparedness and response to a bioterrorist attack, they also introduce liabilities. Dependence on any telecommunication network carries the risk of service failure. Whether from system overload, or coordinated information warfare, denial of service would impact future medical command, control, and response capabilities. Introducing false data could trigger an unnecessary and inappropriate response, and lead to infrastructure collapse. Developers of health information technologies will need to work closely with computer security experts to ensure that products are hardened against cyberterrorism.

References

Centers for Disease Control and Prevention, Electronic Reporting of Laboratory Information for Public Health, Summary of Meeting Proceedings, January 1999, www.cdc.gov/od/hissb/docs.

Centers for Disease Control and Prevention, Bioterrorism Preparedness and Response, www.bt.cdc.gov.

Centers for Disease Control and Prevention, Overview of Epi Info 2000, www.cdc.gov/epiinfo.

Committee on R&D Needs for Improving Civilian Medical Response to Chemical and Biological Terrorism Incidents, Institute of Medicine and National Research Council, Chemical and Biological Terrorism Research and Development to Improve Civilian Medical Response, National Academy Press, Washington, D.C., 1999.

Emergency Management Institute, IS 195, Basic Incident Command System, Federal Emergency Management Agency, 2000, www.fema.gov/emi.

Freimuth V, Linnan HW, Potter P, Communicating the Threat of Emerging Infections to the Public, Emerging Infectious Diseases 2000, 6:337-347.

Kearns, J, Embracing the Era of Internet Health, BT Alex Brown s 1999 Health Care Conference, May 1999, intel.com/intel/e-health/presentations.htm.

Red Herring, Health Care and the Net, pp 199-276, October 2000.

U.S. Congress, Office of Technology Assessment, Bringing Health Care Online: The Role of Information Technologies, OTA-ITC-624, Washington, D.C.: U.S. Government Printing Office, 1995.

Clinical Practice Guideline - Telemedicine in Plastic Surgery

G. Ayorkor Mills-Tettey

Background

Telemedicine is a system of healthcare delivery at a distance by the use of telecommunications technology. It has numerous applications, the most obvious of which include providing healthcare to patients in remote or rural areas, and consulting specialists in distant institutions.

Telemedicine in the United States began with the use of a two-way, closed circuit television link for medical treatment and education, by the University of Nebraska in 1959. Another early application include the joint NASA/U.S. Public health Service/Lockheed Corporation "Space Technology Applied to Rural Papago Advanced Health Care" (STARPAHC) project, a program that brought medical care to remote areas of the Papago Indian Reservation in Arizona in 1970. Following further pioneering work in rural Canada and at the Massachusetts General Hospital in Boston, the first transoceanic telemedicine support system was established by the Naval Ocean Services Center in 1982. This Remote Medical Diagnostic System continues as a vital means of delivering health care to shipboard personnel. Recent advances in fiber optics and digital compression have allowed this technology to become more affordable and widely applicable in clinical medicine, especially in radiology and psychiatry. Today's information revolution has sparked renewed interest in the field of telemedicine.

Activities that fall under the broad umbrella of "Telemedicine", the remote delivery of healthcare, currently take two main forms.

Fully interactive telemedicine involves real time (instantaneous) communication and interaction between a physician and a patient over a telecommunications link that usually consists of a two-way video and audio communication. Such an interaction is similar to videoconferencing that would take place in a business setting. For medical applications however, standards of image, motion, and sound quality are often higher than those required for a typical business videoconference. These standards are determined by the specific application and are related to the amount of information needed for a physician to make a definitive diagnosis. Equipment that would be found on both ends of a typical real-time telemedicine link includes television screens, microphones, and transmission equipment.

The second form of telemedicine is referred to as Store-and-Forward (SAF) Telemedicine. Here, as the name implies, the patient is examined by local health personnel and the relevant information from a patient examination is stored as text, images, or even sound files, and is then forwarded to the consulting specialist at a later time by the use of computers and a telecommunications link. This may be done through a pre-established network, such as a local-area network within an institution, by transmission between two sites using telephones, satellite, radio, microwave links, or the internet.

The main advantage that real-time telemedicine holds over store-and-forward telemedicine is the opportunity it affords for full interaction between the physician and the patient in question. This corresponds closely to the traditional physician's examinations that patients are accustomed to. It also allows physicians to make behavioral observations of a patient. However, due to its technological requirements discussed below, real-time telemedicine often involves very prohibitive costs. For several applications, store-and-forward telemedicine, which is much less costly, is adequate or even preferable. While real time telemedicine necessitates pre-scheduled appointments for the telemedicine session between the two sites, store-and-forward systems can overcome limitations related to time, in addition to geography, because it eliminates the need for scheduling between two sites. Thus, both forms of telemedicine have important uses in different applications.

Diagnosis at a distance is an important application of telemedicine in several fields, including plastic surgery. Treatment planning and monitoring of patients through remote connections may save time, and reduce cost and inconvenience by avoiding the transportation of ill patients and making it possible to consult specialists in different geographic areas. When telemedicine is extended to the home care of patients, it may be possible to reduce the length of hospital stays and provide more consistent monitoring of chronically ill patients without time-consuming and potentially dangerous travel by the patient or physician.

An example of a program that illustrates the remote diagnosis application in plastic surgery and primary health care is the International Medical Electronic Link (IMEL), an internet-based system that allows doctors in remote parts of Peru and Nepal to consult specialists in larger hospitals in the respective countries, and also at the Dartmouth Hitchcock Medical Center the United States. This store-and-forward telemedicine link saves patients expensive travel arrangements and provides support for primary care physicians in these remote areas. Participating physicians are registered at the IMEL website and may request a consultation by selecting the desired department and consultant from a list at the website. The physician then enters the patient's clinical information on a department-specific online consultation form, includes any digitized images, and submits the request. The specialist is notified by e-mail of the requested consultation, and by going to the IMEL website, he can access the patient record, examine the case, and append a response. The primary care physician and specialist may exchange follow-up information in this manner, and a comprehensive electronic case record for each patient is thus maintained. IMEL has proved very effective in surgical planning and diagnosis of diseases.

Yale University, in collaboration with Interplast Organization, effectively used an internet-based system to screen potential plastic surgery candidates in Manaus, Amazonas, Brazil, prior to arriving on-site in 1997. The program was publicized through the news media, and potential patients reported at an oncological hospital in Manaus for a physical examination. A commercially available digital camera (The Color QuickCam by Connectix Inc, 640 by 480 pixels) facilitated imaging. Using a Pentium PC at the Manaus site, an Apple Macintosh at the Yale site, a 22.8 kilobytes per second bandwidth modem, and a local internet service provider, images of the patients along with a bilingual history-physical examination form were sent to Yale by e-mail. The data and images were evaluated by plastic surgeons, pediatricians and anesthesiologists, and the diagnosis and proposed operating procedure and schedule were forwarded back to Manaus. Upon arrival on site, each patient was re-evaluated prior to surgery and for all 99 of the patients scheduled, the diagnosis and treatment plan was in 100 percent agreement with the prior remote evaluation. Evaluating patients over the Internet beforehand saved about 20% of the time spent on-site.

Computers, telecommunications, and biotechnology are some technologies that may be combined into a telemedicine system. The technology that forms the basis of a telemedicine system is the telecommunications link, which serves as the channel through which the audio, visual, and textual data generated in a telemedicine encounter must be relayed. This data may be transmitted as analog (continuos) signals, such as over plain telephone lines, or as digital (discrete) signals, such as through a satellite link. Video and audio signals are analog signals, and in order to relay them over digital transmission systems, they must be converted to digital signals first. In such systems, this conversion is achieved by a Coder/Decoder (Codec), a device that converts an analog signal into a digital signal at its point of transmission and back again at its point of reception. The amount of information per second to be transmitted, or the required bandwidth, determines the telecommunications technology used, from low-bandwidth plain telephone lines to high-bandwidth fiber optic cables and satellite technologies. Real-time interactive telemedicine generally requires high bandwidth communication capabilities due to the large amount of visual and audio information that must be transmitted each second. Store-and-forward systems typically require lower bandwidths. Larger bandwidths used in telemedicine systems relate to higher costs. Because of this, the development of telemedicine is closely linked to the further development of data compression techniques, in which information is compressed in order to be relayed over lower-capacity channels.

Aspirations to develop telemedicine so that it closely mirrors face-to-face medicine, and even to enhance telemedicine beyond the traditional medical experience, have resulted in the development of several highly innovative telemedicine-related technologies. "Digital instruments" such as electronic stethoscopes and digital dermatoscopes can enhance interactive telemedicine systems. In telepathology, robotically controlled microscopes may be used to examine samples at the remote site. The innovation continues into the future; although not in general use today, telesurgery applications employing robotics enhanced with virtual reality are currently being actively experimented with.

Telemedicine raises several interesting questions beyond its strictly medical and technological implications.

Loss of confidentiality is a potential hazard of telemedical communication. The transmission and storage of electronic information pose security concerns that are much greater than those with a paper record. Although encoding technologies are achieving greater sophistication, it is not likely that unauthorized access to private medical information can ever be completely prevented. Methods to enhance security include the use of encryption and the establishment of passwords to log onto network systems.

The defining feature of telemedicine the distance between the patient and physician is a great source of risks related to liability and licensure. Issues of licensure require resolution because medical licenses, granted by individual state boards, make no current provision for electronic patient care from outside their own jurisdictions. Suggested alternatives to full licensure requirements include exceptions for special conditions, exemptions for telemedicine in general, and limited telemedicine licensure. Also unresolved is the question of legal exposure of the telemedical consultant to charges of negligence. It is not established how the traditional standards of the physician-patient contract apply in an electronic communication.

Reimbursement structures must be systematized. Medicaid presently allows states to reimburse for telemedical consultations on an optional basis. Thus far, this provision has been adopted in 14 states: Arkansas, California, Georgia, Iowa, Illinois, Kansas, Louisiana, Montana, North Dakota, Oklahoma, South Dakota, Texas, Virginia, and West Virginia. In addition, Maine, Nebraska, North Carolina and Utah are developing plans to cover telemedicine.

Finally, the day-to-day organization of a telemedicine program raises interesting issues such as the roles of local staff, management, physicians, and HMOs.

Telemedicine is a fast-growing field. Its development and acceptance depend on a favorable demonstration of its performance in relation to traditional approaches to healthcare in several fields. This includes a demonstration of improvements in quality of care provided, of its cost-effectiveness, and of other advantages it offers over face-to-face healthcare delivery. A fast-growing number of researchers and institutions are actively involved in quantifying these attributes through the establishment and evaluation of telemedicine programs. Telemedicine has already proved useful in many rural and remote settings.

BIBLIOGRAPHY & REFERENCES

[1] Preston, Jane, The Telemedicine Handbook, Telemedicine Interactive Consultative Services Inc, 1993

[2] www.i-mel.org

[3] Moncur, Rosen et al, "Medical Electronic Link (MEL): Providing Telemedicine on the World Wide Web", Medicine Meets Virtual Reality: Global Healthcare Grid, Morgan et al (Editors), IOS Press, Netherlands, 1997, pp. 328-333.

[4] Barrett, Randy, "Telemedicine on the rise on the internet", Inter@ctive Week, May 12 1997

[5] "Telemedicine: Low-Bandwidth Applications for Intermittent Health Services in Remote Areas", JAMA, October 21 1998-Vol 280, No. 15

[6] Wolf et al, "Telemicroscopy via the Internet", Nature, Vol. 391 (5 Feb), pp. 613-614
[7] Stava, Richard M., "The virtual surgeon", The Sciences, Vol. 38, No 6, Nov/Dec 1998, pp. 34-9
[8] "A Telemedicine Primer", Practical Lawyer, April 1999
[9] Perlin et al, "Telemedicine", Hospital Physician, 26-34, 36, November 1999, pg. 33
[10]"Medicaid and Telemedicine", Medicaid Policy and Program Information http://www.hcfa.gov/medicaid/telemed.htm, March 1999
[11] Several examples of articles and papers documenting telemedical research, test systems and evaluation are: Bruno et al, "Techniques in Endourology: Digital still image recording during video endoscopy", Journal of Endourology, Vol. 13, No 5, Jun 1999, pp. 353-356
12 Gilbert et al, "NASA/DARPA Advanced Communications Technology Satellite for evaluation of Telemedicine Outreach using next-generation communications satellite technology: Mayo Foundation participation", Mayo Clinic Proceedings, Vol. 74, No 8, August 1999, pp. 753-757
13 Houston et al, "Clinical Consultations Using Store-and-Forward Telemedicine Technology", Mayo Clinic Proceeding, August 1999, pp. 764-769
14 Julsrud et al, "Telemedicine Consultations in Congenital Heart Disease: Assessment of Advanced Technical Capabilities", Mayo Clinic Proceedings, Vol. 74, No 8, August 1999, pp. 758-763
15 Mattioli et al, "Technical Validation of Low-Cost Videoconferencing Systems Applied in Orthopedic Teleconsulting Services, Computer Methods and Programs in Biomedicine, Vol. 60, No. 2, Sept 1999, pp. 143-152
16 Rosser et al, "Use of Mobile Low-Bandwidth Telemedical Techniques for Extreme Telemedicine Applications", Journal of the American College of Surgeons, Vol. 189, No 4, October 1999, pp. 397-404
17 Shimizu Koichi, "Telemedicine by Mobile Communication: Techniques for Multiple Data Transmission from Moving Vehicles in Emergency Medicine Situations", IEE Engineering in Medicine and Biology, July/August 1999, pp. 32 - 44
18 Stamford et al, "The Significance of Telemedicine in a Rural Emergency Department: Studying the Impact that Linking a Major Medical Center to a Rural Hospital Has on Treatment in Remote Areas", IEE Engineering in Medicine and Biology, July/August 1999, pp. 45-52
19 Tekeda et al, "High Quality Image-Oriented Telemedicine with Multimedia Technology", International Journal of Medical Informatics, Vol. 55, No 1, Jul 1999, pp. 23-31
20 Whited et al, "Reliability and Accuracy of Dermatologists Clinic-Based and Digital-Image Consultations", Journal of the American Academy of Dermatology, Vol. 41, No 5 (part 1 Nov 1999) pp. 693-702

Persistence of Native and Non-indigenous Microorganisms in Winter Conditions

Mike Reynolds, Ph.D.

Background:

We are investigating the natural or enhanced "recovery ability" or decontamination of soil following exposure to selected non-indigenous organisms and toxic chemicals. Our group's background is in soil microbiology, soil chemistry, and modeling, particularly in cold regions or winter conditions. In our research, we treat the soil as a system that contains not only microbiology, but also chemical, physical, climatic, and vegetation related influences. In the environmental quality arena, we have been investigating low-cost, biologically-driven methods of decontaminating soils following releases of military and industrial chemicals. Mechanistically, we are modifying the dominant soil microbial community and activity to favor the desired pathways. Our approach is to treat the soil as a system that contains not only microbiology, but also chemical, physical, climatic, and vegetation-related influences. The basic premise of favorably altering the soil microbiology can be transferred to address the "recovery ability," or decontamination, of soil following release of chemical and foreign organisms biological agents.

Issues:

We have a new effort to understand the persistence and fate of biological foreign agents microorganisms that may be released, especially in a cold or winter setting. We are working with endospore-forming bacteria. Although there are decontamination approaches for hard non-porous surfaces, these approaches, that are often based on oxidation, are much less successful in treating soil, due to the competition from other oxidizable compounds in the soil. Endospores are undoubtedly persistent in a cold soil. We are seeking to better understand and then alter the potential risk associated with a soil that has been inoculated with endospores. Questions that appear important include:

- How and for how long, would endospore-inoculated soil affect civilian and military activities?
- Can endospore numbers be reduced sufficiently for different military, civil defense, and civilian activities to resume?
- How do we effectively reduce endospore numbers?
- What is the importance of soil properties and environmental conditions, such as snow or ice cover, in predicting decay (or growth) of endospore-forming bacterial communities?
- Can we predict endospore fate following thawing, or during the numerous freeze-thaw cycles that occur at the soil surface during the spring? Does the indigenous microbial population have a competitive advantage over introduced microorganisms and can we capitalize on that?(Our initial data suggest this.)

- What are the influences of bioavailable nutrients and water?
- Can we modify soil conditions on a large scale to maximize the die-off of non-indig nous, endospore-forming bacteria in soil?
- Can we somehow prime or precondition high-threat areas of soil?
- Can this information be coupled with intelligence sources, perhaps via a GIS-based system, in a way that best enables our response or best focuses our resources?

Approach:

We are in the early stages of investigating the potential of altering a soil's microbial community to maximize the competitive advantage of native microorganisms over introduced microorganisms. Ideally, we would maximize competition to coincide with the germination of non-indigenous endospores, and from this, maximize the die-off of introduced pathogens.

To address this, we are using knowledge and capabilities gained from our previous research efforts that have centered on biological treatment, or bioremediation, of soil contaminated with organics. In brief, we have found that we can alter the soil microbial community structure by low-cost, readily implemented actions that are applicable over large areas, and in doing this we can influence the dominant processes in the soil. The complexity of the soil system and the relative difficulty in characterizing soil microbial communities makes it difficult to confirm that we have successfully changed the community structure. We are using fatty-acid- and phospholipid-fatty-acid-based techniques to characterize soil microbial communities.

Our rationale for using an approach based on biological competition is based on our experience with treating soils contaminated with organic compounds. One simplified view of the evolution of accepted options for treating soil contaminated with organic compounds is that we have gone from brute-force-but-easy-to-understand to complex-but-very-effective technologies. That is, we have gone from:

- Thermal oxidation, "dig it up and burn it," to
- Chemical oxidation, "dig it up and wash it with a strong oxidant," to
- Biological oxidation, "dig it up and put it in a bioreactor," to
- Natural attenuation, "natural processes will remediate many sites," and finally to
- Enhanced natural remediation, let's understand the system so we can manipulate it to give natural processes a significant boost.

The latter is the approach we have taken with organic contaminants in soil and are investigating for use with foreign microorganisms that may be viewed as "biological contaminants".

Conclusion

Joseph Rosen, MD

This report has provided a view of emerging technologies as tools for counterterrorism. It has also considered emerging technologies as new weapons for terrorists especially as weapons of mass destruction. Differing from other reports, it has attempted to put these new responses and weapons into the context of our present strategies and operational plans. It also emphasizes the importance of balancing our strategies and plans against the ones that terrorists use.

To create a strategy to combat terrorism, we must first understand the terrorist strategy. In the words of Sun Tzu written over 2,500 years ago, If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Our pattern over the past ten years has been one of terrorist attack and counterterrorist response. We must therefore be prepared for further terrorist attacks   attacks that may cross a threshold and begin to use weapons of mass destruction. These groups may be domestic or international, and the attacks may be against civilian or military targets, either at home or abroad. There are no longer the 20^{th} century borders that have protected the US from attack on our own shores and these borders will continue to disappear in both our physical and cyberspace worlds. The US is not in a position with respect to our government, our freedoms, or our culture, to recreate these walls. Our free society makes us exceeding vulnerable to attack, and our position in the world makes us the primary target for many groups.

The goal and overarching recommendation is prevention of terrorist attacks. We hope that this can be achieved through our suggestions and the suggestions of others. However, neither the present time, nor in the future should we underestimate the capabilities of terrorist groups to carry out their policies and operational plans to cause large mass casualties in the continental US using either conventional weapons in unconventional ways or weapons of mass destruction. In our war of numbers we have shown that our policies and operations may decrease the number of attacks, but that the violence of these attacks has not decreased. As terrorists cross the threshold and use weapons of mass destruction, we should be prepared to meet this new possible challenge.

Our overarching recommendation is a national counterterrorist response simulation center, that is distributed throughout the country, and will prepare the country to respond to a mass casualty, and wide spread strategic attack in a comprehensive and successful manner. At present, a large-scale bioweapons attack with or without a cyberattack would overwhelm our current operational plans. With training and continued implementation of emerging technologies, these operational plans can be rapidly improved to respond to weapons of mass destruction, including bioweapons. This simulation center, based on virtual reality, could provide this environment for training, education, and practice.

In addition, this simulation environment would provide a unique tool to bring together policy makers, operational players and technologists to interact in constructive ways that would help our approach evolve according to the changing strategies, operational plans, and tools that are being used by the terrorists. Although at present there are numerous conferences and round table meetings that bring together some of the people and elements of our counterterrorist effort, the environment in which they meet is not necessarily conducive to rapid change in response to the new threats that the terrorist poses to our society.

In addition to the value of the distributed simulation system, the virtual reality training center would also provide a network of nodes that could be used in the event of a real attack. It would provide the infrastructure to begin to put into place a widespread mesh (see National Defense University book cited in recommended reading section) that could operate during an attack to bring together the necessary personnel and materials to respond to a large-scale attack. It would provide an environment in which we could train as we fight and fight as we train. It would give all levels of the inter-agency plans a chance to engage in simulated attacks and create relationships between the many agencies and individuals on which we will depend when a large-scale mass casualty event occurs. This approach has been used successfully in both the civilian and military communities.

During our conference we presented an attack on Hanover, New Hampshire, the location of Dartmouth College and our Institute. We presented this attack as if it were in the present (2000 - 2005), and also in a future framework (beyond 2005, up to 2025). In the present attack, a bioweapon (pneumonic plague) was used which would rapidly spread to other cities. This bacteria presently has a definite medical response. We calculated possible scenarios with differing levels of infection. We then examined, in detail, the resources in our region to respond to these differing levels. We examined the command and control, the timing of response, and how effective the inter-agency plans would be in responding to this threat. We then examined a similar attack on Hanover, but in the future, in which a bioagent had been bioengineered to not have a readily available vaccine or treatment (see edited volume).

In both cases, the resources needed would rapidly overwhelm the ones locally available. The response would require a major medical first responder operation that is presently lacking. It would also require a quarantine, that even for the defense department would be a very challenging task to implement. We attempted to run this scenario with people representing each of the true agencies that would respond according to the guidelines that they need to follow. We were sensitive to issues of lead federal agency, FBI, and to the timeline that we were working against. The goal was not to demonstrate what worked and what did not work, but rather to demonstrate how complex this scenario would rapidly become for all involved in the operational plan.

The simulation approach that we recommend is neither a top-down or bottom-up approach. It is not directed at any one geographic area over another. Rather, it would integrate all of the elements, and allow us to modify and train for mass casualty events that could spread rapidly from city to city and affect (infect) a large percentage of the population. Although we can argue over whether a certain bioagent (i.e. smallpox) will infect 10% or 30% of a city population, in either case, the numbers rapidly overwhelm our present medical facilities. In both cases, the present medical facilities and infrastructure are not prepared to meet either challenge with or without further degradation from a cyberthreat launched with a biothreat. Our present infrastructure, whether it be information or physical, is not prepared for this threat either.

We believe that scenarios like this are realistic and will allow us to prepare for these events. They will also allow us to better prepare for smaller scale events that will continue to occur (though we hope more infrequently in the future). The national response simulation center could test a national response system and validate what works and invalidate what does not. It could test alternate response strategies and provide a national distributed command and control system into which each of the operational players could be integrated, and trained in on a regular basis.

Specifically, with respect to US bioweapons preparedness, this national response simulation center could conduct multiple scenarios that identify resource availability, movement and timing of resources, and the best utilization of command and control strategies. The interplay of local and state resources, with federal agencies from both the justice department and the defense department have to be trained for these large scale, multi-state and city, mass casualty events before they take place. This would enable us to minimize the damage incurred by this type of attack.

Although we hope that our strategy and policy will create a world in which we never have to sustain another terrorist attack either in the US or against US personnel abroad, we do not believe that this is a realistic assumption. The trend has been otherwise over the past decade and recent events have shown the capacity of terrorists to strike our most vital assets both physically and in cyberspace. We are recommending an approach that will provide tools to complement and augment the ones that the FBI and the department of justice already have in place. The tools that we provide will help to educate and train personnel, and eventually perform the tasks involved in the successful implementation of our operational plans to respond to counterterrorist attacks in the future. They will enable us to modify our plans when emerging threats appear, and to rapidly introduce emerging technologies to help counteract them. The national response simulation center will be an important tool in facing the challenge of terrorism to the American society in the 21st century.

Terms and Definitions

The terms and definitions have been included from the Federal Response Plan[1] for three reasons:

1.) It will enable the reader of our report to have a single comprehensive source of defi nitions and acronyms that are commonly used in disaster relief and response to terrorist incidents.
2.) The terms and definitions will give the reader a notion of how overwhelming the task is to fully comprehend all the elements that have to be coordinated during a terrorist inci dent. This includes agencies, people, timelines, and other logistical support.
3.) The purpose of this report is to look at ways to better integrate and streamline the response plan.

Accountable Property: Property that (a) has an acquisition cost of $15,000 or more; (b) has a unique, identifiable serial number (e.g., computer or telecommunications equipment); or (c) is considered "sensitive" (i.e., easily pilfered), such as cellular phones, pagers, and laptop computers.
Action Plan: A verbal or written plan reflecting FCO/State Coordinating Officer priorities with tactical objectives for the next operational period.
Aerial Port of Debarkation: Arrival airfield in or near the area affected by the disaster or emergency. In the National US&R Response System, also known as the Point of Arrival.
Aerial Port of Embarkation: Departure airfield in the vicinity of a US&R task force s home base. In the National US&R Response System, also known as the Point of Departure.
After-Action Report: Following Federal response to a disaster under the FRP, FEMA will coordinate an after-action report documenting the Federal response effort. Each Federal agency involved in the response will keep records of its activity to assist in preparing the after-action report.
Agency Logistics Center (ALC): An organization that provides centralized control, transportation, deployment, and accountability of all disaster support goods within the TLC network. The ALC was developed to enhance readiness and response, improve accountability of disaster assets, and reduce overall disaster costs.
Assembly Point: A designated location for responders to meet, organize, and prepare their equipment prior to moving to the Point of Departure. Since emergency teams, organizations, and resources involved in a disaster or emergency can originate from a variety of geographic locations, each typically has its own Assembly Point.
Asset Visibility: Monitoring of the inventory levels of all goods that can be used for disaster operations that are in storage sites and of their movements to designated locations. Resource tracking is a subcomponent of asset visibility since it views only a subset of the overall inventory and tracks assets as they are applied to a specific disaster.
Assets: See Resources.

1. Federal Emergency Management Agency (FEMA): Incident Annexes to the Federal Response Plan, April 1999, http://www.fema.gov/r-n-r/frp/frpterr.htm

Base Camp: The designated location under local or State control within the disaster area that is equipped and staffed to provide sleeping facilities, food, water, and sanitary services to response personnel.
Base Support Installation: Any military installation of any service or agency designated by the Department of Defense to provide civil authorities with specified, integrated support of disaster operations. The installation is normally located outside, but within relative proximity to, the disaster area.
Biological Agents: The FBI WMD Incident Contingency Plan defines biological agents as microorganisms or toxins from living organisms that have infectious or noninfectious properties that produce lethal or serious effects in plants and animals.
Catastrophic Disaster Response Group: The CDRG, composed of representatives from all FRP signatory departments and agencies, operates at the national level to provide guidance and policy direction on response coordination and operational issues arising from the FCO and ESF response activities. CDRG members are authorized to speak for their agencies at the national policy level. During a disaster the CDRG convenes as necessary, normally at FEMA Headquarters; the EST provides any needed support.
Chemical Agents: The FBI WMD Incident Contingency Plan defines chemical agents as solids, liquids, or gases that have chemical properties that produce lethal or serious effects in plants and animals.
Civil Air Patrol: **a.** Provide a liaison to the DFO to work with the Operations and ESF #5 Sections to facilitate coordination of Civil Air Patrol (CAP) support operations and to ensure that CAP activities are reported in the SITREP. Input to the SITREP also may be submitted through the Defense Coordinating Element. **b.** Designate an appropriate CAP Wing Staff person to coordinate CAP-FEMA planning and response activities between the CAP-U.S. Air Force region and the FEMA regional staff.
Civil Transportation Capacity: The total quantity of privately owned transportation services, equipment, facilities, and systems from all transport modes nationally or in a prescribed area or region.
Comprehensive Environmental Response, Compensation, and Liability Act, as amended (CERCLA): More popularly known as "Superfund," CERCLA was passed to provide the needed general authority for Federal and State governments to respond directly to hazardous substances incidents.
Congressional Affairs Representative: Initial and continuing actions of agency CARs include: **(a)** Support the DCLO in establishing priorities, preparing notification statements for DCLO approval, making congressional notification calls, providing feedback on congressional reaction, etc.; **(b)** Establish contact with operational staff or ESF agencies and monitor ESF activities; **(c)** Maintain input to congressional inquiry and notification tracking systems; and **(d)** Respond in a timely fashion to congressional inquiries pertaining to the ESF of responsibility.
Congressional Relations Officer (CRO): designated by the Director, FEMA Office of Congressional and Legislative Affairs. The CRO is located at FEMA Headquarters and is a member of the Emergency Support Team (EST)
Consequence Management:

1. **Pre-Release**

a. FEMA receives initial notification from the FBI of a credible threat of terrorism.
Based on the circumstances, FEMA Headquarters and the responsible FEMA region(s)

may implement a standard procedure to alert involved FEMA officials and Federal agen cies supporting consequence management.

b. FEMA deploys representatives with the DEST and deploys additional staff for the JOC, as required, in order to provide support to the FBI regarding consequence manage ment. FEMA determines the appropriate agencies to staff the JOC Consequence Management Group and advises the FBI. With FBI concurrence, FEMA notifies conse quence management agencies to request that they deploy representatives to the JOC. Representatives may be requested for the JOC Command Group, the JOC Consequence Management Group, and the JIC.

c. When warranted, FEMA will consult immediately with the Governor s office and the White House in order to determine if Federal assistance is required and if FEMA is per mitted to use authorities of the Robert T. Stafford Disaster Relief and Emergency Assistance Act to mission-assign Federal consequence management agencies to pre-deploy assets to lessen or avert the threat of a catastrophe. These actions will involve appropriate notification and coordination with the FBI, as the overall LFA.

d. FEMA Headquarters may activate an Emergency Support Team (EST) and may con vene an executive-level meeting of the Catastrophic Disaster Response Group (CDRG). When FEMA activates the EST, FEMA will request FBI Headquarters to provide liai son. The responsible FEMA region(s) may activate a Regional Operations Center (ROC) and deploy a representative(s) to the affected State(s). When the responsible FEMA region(s) activates a ROC, the region(s) will notify the responsible FBI Field Office(s) to request a liaison.

2. Post-Release:

a. If an incident involves a transition from joint (crisis/consequence) response to a threat of terrorism to joint response to an act of terrorism, then consequence management agencies providing advice and assistance at the JOC pre-release will reduce their pres ence at the JOC post-release as necessary to fulfill their consequence management responsibilities. The Senior FEMA Official and staff will remain at the JOC until the FBI and FEMA agree that liaison is no longer required.

b. If an incident occurs without warning that produces major consequences and appears to be caused by an act of terrorism, then FEMA and the FBI will initiate consequence management and crisis management actions concurrently. FEMA will consult immedi ately with the Governor s office and the White House to determine if Federal assistance is required and if FEMA is permitted to use the authorities of the Stafford Act to mis sion-assign Federal agencies to support a consequence management response. If the President directs FEMA to implement a Federal consequence management response, then FEMA will support the FBI as required and will lead a concurrent Federal conse quence management response.

c. The overall LFA (either the FBI or FEMA when the Attorney General transfers the overall LFA role to FEMA) will establish a Joint Information Center in the field, under the operational control of the overall LFA s Public Information Officer, as the focal point for the coordination and provision of information to the public and media concern ing the Federal response to the emergency. Throughout the response, agencies will con tinue to coordinate incident-related information through the JIC. FEMA and the FBI will ensure that appropriate spokespersons provide information concerning the crisis manage ment and consequenct management responses. Before a JIC is activated, public affairs offices of responding Federal agencies will coordinate the release of information through the FBI SIOC.

d. During the consequence management response, the FBI provides liaison to either the ROC Director or the Federal Coordinating Officer (FCO) in the field, and a liaison to the EST Director at FEMA Headquarters. While the ROC Director or FCO retains authority to make Federal consequence management decisions at all times, operational decisions are made cooperatively to the greatest extent possible.

e. As described previously, resolution of conflicts between the crisis management and consequence management responses will be provided by the Senior FEMA Official and the FBI OSC at the JOC or, as necessary, will be obtained from higher authority. Operational reports will continue to be exchanged. The FBI liaisons will remain at the EST and the ROC or DFO until FEMA and the FBI agree that a liaison is no longer required.

3. Disengagement

a. If an act of terrorism does not occur, the consequence management response disen gages when the FEMA Director, in consultation with the FBI Director, directs FEMA Headquarters and the responsible region(s) to issue a cancellation notification by standard procedure to appropriate FEMA officials and FRP agencies. FRP agencies disengage according to standard procedure.

b. If an act of terrorism occurs that results in major consequences, each FRP component (the EST, CDRG, ROC, and DFO if necessary) disengages at the appropriate time accord ing to standard procedure. Following FRP disengagement, operations by individual Federal agencies or by multiple Federal agencies under other Federal plans may continue, in order to support the affected State and local governments with long-term hazard mon itoring, environmental decontamination, and site restoration (cleanup).

Contingency Plan: Targets a specific issue or event that arises during the course of disaster operations and presents alternative actions to respond to the situation.

Credible Threat: The FBI conducts an interagency threat assessment that indicates that the threat is credible and confirms the involvement of a WMD in the developing terrorist incident.

Crisis Management: The FBI defines crisis management as measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

Defense Coordinating Officer (DCO): **(a)** Is the designated DOD on-scene member of the ERT; **(b)** Coordinates RFAs and mission assignments with the FCO or designated representative, normally the ERT Operations Section Chief; and **(c)** Is supported on scene by a Defense Coordinating Element (DCE), composed of administrative staff and liaison personnel, including the Emergency Preparedness Liaison Officer (EPLO), who normally will collocate with the ERT Operations Section.

Designated Agency Safety and Health Official (DASHO): The individual who is responsible for the management of the occupational safety and health program within an agency, and is so designated or appointed by the head of the agency. The DASHO is the agency s policy-level advocate for the safety and health of its personnel.

Designated Area: The geographic area designated under a Presidential major disaster declaration that is eligible to receive disaster assistance in accordance with the provisions of the Stafford Act.

Direct Federal Assistance: Is provided to the affected State and local jurisdictions when they lack the resources to provide specific types of disaster assistance either because of the specialized nature of the assistance, or because of resource shortfalls (e.g., providing debris removal, potable water, emergency medical services, and urban search and rescue).

Disaster Field Office: The DFO is the primary field location in each affected State for the coordination of Federal response and recovery operations. It operates 24 hours per day, as needed, or under a schedule sufficient to sustain Federal operations. The FCO and SCO collocate at the DFO, along with Federal agency regional representatives and State and local liaison officers, when possible. Once the DFO is ready for use, the ERT-A and/or ERT-N is augmented by FEMA and other Federal agency staff to form a full ERT.

Disaster Finance Center: The OFM/DFC, located in Berryville, VA, will:

1. Process all DRF payments;
2. Serve as the point of contact for inquiries relating to bill processing and payments;
3. Receive and review bills prior to processing payments to ensure that proper documen tation supports the expenditures claimed;
4. Initiate chargebacks to FEMA s account for On-Line Payments and Collections (OPAC) system payments that are not supported with documentation;
5. Perform periodic reviews of open obligations to ensure accuracy and timeliness;
6. Provide financial management reports on DRF activities;
7. Track emergency aid (identified on the RFA) and bill the State cost-share portions; and
8. Track and initiate closeout procedures for each mission assignment.

Disaster Information Systems Clearinghouse (DISC): An organization that provides centralized control, deployment, and accountability of disaster information systems. The DISC is located at FEMA s Mount Weather Emergency Assistance Center in Bluemont, VA.

Disaster Medical Assistance Team (DMAT): The basic deployable unit of the National Disaster Medical System, which is administered by the Department of Health and Human Services. Staffed with physicians, nurses, other health care professionals, and support staff, DMAT capabilities include triage and stabilization of patients at a disaster site and provision of austere medical services at transfer points during transport to definitive medical care locations.

Disaster Mortuary Team (DMORT): Assist in providing victim identification and mortuary services

Disaster Recovery Center (DRC): A Disaster Recovery Center (DRC) is a centralized location where individuals affected by a disaster can go to obtain information on disaster recovery assistance programs from various Federal, State, and local agencies as well as voluntary organizations. Trained staff also is on hand to provide counseling and advice. It is generally expected that individuals visit the DRC after they have called the teleregistration center to apply for assistance, as applications usually will not be taken at the DRC. However, a DRC may serve as a workshop site for assisting families and businesses to complete Small Business Administration disaster loan application forms. A center dealing only with mitigation in reconstruction and rebuilding techniques may be called a Reconstruction Information Center (RIC). A RIC may be set up at a fixed or mobile location.

Federal Coordinating Officer/Disaster Recovery Manager: The FCO/DRM is delegated authority by the Regional Director to exercise the authority vested in the RD for a major disaster or emergency. Therefore, all of the financial authorities vested in the RD are vested in the FCO/DRM. The FCO/DRM can delegate authority for approval of specific financial management transactions to other FEMA officials.

1. The FCO/DRM is responsible for project management, which may be delegated to designated Project Officers. For procurement of equipment and supplies, the Logistics Section will provide Project Officers, unless otherwise agreed upon between the Logistics Section Chief, the Comptroller, and the mission-assigned agency.

2. FEMA officials who are delegated mission assignment signature authority are referred to as Federal Approving Officials (FAOs). In addition, every MA has a designated Project Officer, who is responsible for performing project management responsibilities on behalf of the FCO/DRM.

Disaster Response Support Facility (DRSF): A storage facility located near each FEMA MERS detachment, which houses MERS vehicles and associated disaster support materiel.

Disaster Safety Officer (DSO): The DSO will implement a system to report, investigate, and recommend remediation for accidents, injuries, and illnesses related to the disaster or the exercise. This system should include centralized collection and maintenance of safety- and health-related documentation and records. Workers compensation reports may contribute to the reporting system but should not be construed as sole fulfillment of this requirement; and the DSO will provide written evaluations, after-action reports, and exit reports on the disaster safety and health activities. The DSO will include input from other agency safety personnel as appropriate.

Disaster Transportation Management System (DTMS): provides a structure for managing the acquisition of transportation services and the deployment of relief and recovery resources from around the Nation into the disaster area. The DTMS includes two components:

a. TPFDLs, which are planned, prioritized lists of the most critical Federal assets to be deployed rapidly to the disaster site; and

b. Movement Coordination Center(s) to assist in the procurement of transportation assets and track the movement of resources to the disaster area. The MCC team is led by DOT and includes representatives from the Department of Defense (DOD), FEMA, General Services Administration (GSA), and Forest Service. All FRP agencies must notify the MCC when transportation arrangements are made, so that resources can be tracked and reception plans executed.

District Response Group: Established in each USCG District, the District Response Group is primarily responsible for providing the OSC with technical assistance, personnel, and equipment during responses typically involving marine zones.

Domestic Emergency Support Team (DEST): PDD-39 defines the DEST as a rapidly deployable interagency support team established to ensure that the full range of necessary expertise and capabilities are available to the on-scene coordinator. The FBI is responsible for the DEST in domestic incidents.

Donations Coordination Center: Facility from which the Donations Coordination Team operates. It is best situated in or close by the State Emergency Operations Center for coordination purposes. It must have enough rooms for a phone bank, processing by team members of calls from prospective donors, and negotiating the shipping and receiving of needed items.

Donations Coordination Team: A Donations Coordination Team is made up of representatives of voluntary organizations and State and local governments who have a vested interest in the effective management of unsolicited donated goods and voluntary services. The team is managed by the State emergency management agency. Its mission is to implement the State Donations Management Plan, with the aim of keeping unneeded goods and services out of the disaster area.

DOT Crisis Coordinator: A senior-level official appointed by the Secretary of Transportation to manage the Department s emergency response operations during a situation having significant impact upon civil transportation capacity or the transportation infrastructure. For disasters, the Administrator, Research and Special Programs Administration, will normally serve as Crisis Coordinator.

Emergency Response Team: The ERT is the principal interagency group that supports the FCO in coordinating the overall Federal disaster operation. Located at the DFO, the ERT ensures that Federal resources are made available to meet State requirements identified by the SCO. The size and composition of the ERT can range from FEMA regional office staff who are primarily conducting recovery operations to an interagency team having representation from all ESF primary and support agencies undertaking full response and recovery activities. The ERT organizational structure, encompassing the FCO s support staff and four main sections (Operations, Information and Planning, Logistics, and Administration).

Emergency Response Te a m Advance Element: The ERT-A is the initial Federal group that responds to an incident in the field. It is headed by a team leader from FEMA and is composed of FEMA program and support staff and representatives from selected ESF primary agencies. A part of the ERT-A deploys to the State Emergency Operations Center (EOC) or to other locations to work directly with the State to obtain information on the impact of the event and to identify specific State requests for Federal response assistance that are called back to the ROC for processing. Other elements of the ERT-A (including MERS personnel and equipment) deploy directly to or near the affected area to establish field communications, locate and establish field facilities, and set up operations. The ERT-A identifies or validates the suitability of candidate sites for the location of mobilization center(s) and the DFO.

Emergency Support Functions

a. The FRP employs a functional approach that groups under 12 ESFs the types of direct Federal assistance that a State is most likely to need (e.g., mass care, health and medical services), as well as the kinds of Federal operations support necessary to sustain Federal response actions (e.g., transportation, communications). ESFs are expected to support one another in carrying out their respective missions.

b. Each ESF is headed by a primary agency designated on the basis of its authorities, resources, and capabilities in the particular functional area. Other agencies have been des ignated as support agencies for one or more ESFs based on their resources and capabili ties to support the functional area(s).

c. Federal response assistance required under the FRP is provided using some or all of the ESFs as necessary. FEMA will issue a mission assignment to task a primary agency for necessary work to be performed on a reimbursable basis. The primary agency may in turn task support agencies if needed. Specific ESF missions, organizational relationships, response actions, and primary and support agency responsibilities are described in the ESF annexes to the FRP. In cases where required assistance is outside the scope of an ESF, FEMA may directly task any Federal agency to bring its resources to bear in the dis aster operation.

d. Requests for assistance from local jurisdictions are channeled to the SCO through the designated State agencies in accordance with the State emergency operations plan and then to the FCO or designee for consideration. Based on State-identified response requirements and FCO or designee approval, ESFs coordinate with their counterpart State agencies or, if directed, with local agencies to provide the assistance required. Federal fire, rescue, and emergency medical responders arriving on scene are integrated into the local ICS structure.

Emergency Support Function Leaders Group (ESFLG): The principal body that addresses FRP planning and implementation at the working level. It handles issue formulation and resolution, review of after-action reports, significant changes to FRP planning and implementation strategies, and other FRP-related operational issues that involve interagency resolution. The ESFLG forwards to the CDRG issues that cannot be resolved at the working level. Federal agencies designate representatives to serve on the CDRG, ESFLG, and other interagency bodies and working groups. Agencies also participate in FRP exercise, training, and postevent evaluation activities.

Emergency Support Team: The EST is the interagency group that provides general coordination support to the ROC staff, ERT-A, and ERT response activities in the field. Operating from the FEMA Emergency Information and Coordination Center (EICC) in Washington, DC, the EST is responsible for coordinating and tracking the deployment of Initial Response Resources, DFO kits, Disaster Information Systems Clearinghouse (DISC) packages, and other responder support items to the field. The EST serves as the central source of information at the headquarters level regarding the status of ongoing and planned Federal disaster operations. The EST attempts to resolve policy issues and resource support conflicts forwarded from the ERT. Conflicts that cannot be resolved by the EST are referred to the CDRG. The EST also provides overall resource coordination for concurrent multi-State disaster response activities. ESF primary agencies send staff to the EST or opt to coordinate response support activities from their own agency EOCs. It parallels the ERT organization, but is not identical.

Emergency: As defined in the Stafford Act, an emergency is any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property, public health, and safety, and includes emergencies other than natural disasters.

Environmental Response Team: Established by EPA, the Environmental Response Team includes expertise in biology, chemistry, hydrology, geology, and engineering. The Environmental Response Team provides technical advice and assistance to the OSC for both planning and response to discharges and releases of oil and hazardous substances into or threatening the environment.

Essential Elements of Information (EEIs): To assess quickly and accurately the effect of a disaster on the population and infrastructure of an area, emergency managers require early intelligence on the areas noted below. This information facilitates accurate assessment of what response activities and materiel are required to save lives, relieve human suffering, and expedite response and recovery operations. During the early hours of a disaster and in the absence of "ground truth" information such as actual on-site surveys or imagery, GIS, computerized predictive modeling, and damage estimation software may be used to develop initial estimates of damage. As soon as possible, actual on-site ground surveys will be performed. Sources may include a Federal-State Preliminary Damage Assessment and information from Federal, State, and local government agencies, among others, to establish "ground truth" for EEIs as needed.

Federal Coordinating Officer (FCO): Responsible for coordinating the timely delivery of Federal disaster assistance to the affected State, local governments, and disaster victims. In many cases, the FCO also serves as the Disaster Recovery Manager (DRM) to administer the financial aspects of assistance authorized under the Stafford Act. The FCO works closely with the State Coordinating Officer (SCO), appointed by the Governor to oversee disaster operations for the State, and the Governor s Authorized Representative (GAR), empowered by the Governor to execute all necessary documents for disaster assistance on behalf of the State.

Federal Emergency Support Coordinator (FESC): The FESC is the principal point of contact between GSA and FEMA for the establishment of support priorities, allocation of GSA resources, and coordination of the delivery of all GSA equipment, services, and materials except those pertaining to telecommunications. The FESC, with appropriate GSA support staff as determined by the FESC, will normally be located at the DFO. However, at the discretion of the FCO, support may be provided from an already established GSA office, granted that such support is not delayed. The FESC serves until released by the FCO.

Federal Operations Support: Is available to FEMA or other Federal responding agencies when they require logistical or technical support of their Federal operations ESF activation, personnel for preparing damage survey reports, supplies, and equipment for DFO and DRC operations.

Federally Arranged Transportation Support: The identification of available civil transportation capacity, and assistance in procuring such capacity, in support of Federal agencies, State and local governmental entities, and voluntary organizations unable to obtain required services through normal procurement channels.

FEMA Voluntary Agency Liaison (VAL): Each FEMA region has, and FEMA offices in Hawaii and Puerto Rico have, a FEMA VAL. There is also a VAL at the National Emergency Training Center in Emmitsburg, MD. The VAL is responsible for providing advice on voluntary organization coordination and assisting States in developing State Voluntary Organizations Active in Disaster (VOAD). In disaster operations, the VAL assists the local leadership in convening broad-based meetings at which voluntary organizations, FEMA, and the State share information about the status of response and recovery activities.

Fire Suppression Support Coordinator: The person representing ESF #4 at the DFO.

Food and Nutrition Service (FNS) Disaster Task Force: The Food Security Act of 1985 (Public Law 99-198) requires the Secretary of Agriculture to establish a Disaster Task Force to assist States in implementing and operating various disaster food programs. The FNS Disaster Task Force coordinates the FNS overall response to disasters and emergencies. It operates under the general direction of the Administrator of FNS. The FNS Disaster Task Force consists of the Administrator, Associate Administrator, Disaster Coordinator, Deputy Administrator for Management, Deputy Administrator for Governmental Affairs and Public Information, representatives from the food stamp and special nutrition programs, and representatives from regional office(s) affected by the disaster. The FNS Disaster Task Force expedites approval of disaster designation requests and policy clarifications. It also maintains liaison with FEMA Headquarters.

Functional Plan: A subset of the action plan developed by individual elements, setting out their operational priorities for addressing the most pressing problems.

Goods: Equipment and supplies.

Governor s Authorized Representative (GAR): Empowered by the Governor to execute all necessary documents for disaster assistance on behalf of the State.

Hazardous Materials: Under this ESF, hazardous materials are defined broadly to include oil, CERCLA hazardous substances, pollutants and contaminants as defined in CERCLA section 101(33), and certain chemical and biological WMD. Federal response to hazardous materials is carried out under the NCP.

Hazardous Substances: Under this ESF, hazardous substances are defined by section 101(14) of CERCLA.

Incident Command System (ICS): An on-site incident management system applicable to all types of emergencies. Includes standard organizational structure, agency qualifications, training requirements, procedures, and terminology enabling participating agencies to function together effectively and efficiently.

Incident Support Team (IST): An overhead team used to conduct needs assessments, provide technical advice and assistance to State and local government emergency managers, coordinate the activities of multiple US&R task forces in the field, and provide logistical support for US&R task forces beyond their initial 72-hour period of self-sufficiency. The IST reports to the ESF #9 Leader on the ERT.

Incident Support Te a m Advance Element (IST-A): An advance element of the IST, utilized to conduct needs assessments, provide technical advice and assistance to State and local government emergency managers, and prepare for incoming US&R task force and IST resources. The IST-A reports to the IST Commander.

Information Coordination Unit (ICU): A FEMA Headquarters team that monitors and reports daily on potential or actual disasters. Prior to an incident, the ICU provides daily situation updates about all ongoing or pending activities. During a disaster, ICU members become part of the EST Information and Planning Section, Situation Status Branch.

Initial Response Resources (IRR): Critical goods provided to victims and all levels of government responders immediately after a disaster occurs. IRR goods are used to augment State and local capabilities. FEMA s Logistics Division is responsible for storing and maintaining a limited quantity of critical IRR goods, initiating the acquisition of nonstocked items through Federal logistics partners, and pre-positioning equipment and supplies when required. IRR goods include equipment (e.g., emergency generators and refrigerated vans) and supplies (e.g., food, water, and personal hygiene items).

In-Kind Donations: Donations other than cash (usually materials or professional services) for disaster survivors.

Joint Information Center (JIC): Provides a central point for coordinating emergency public information activities.

Joint Operations Center (JOC): When a Joint Operations Center (JOC) is formed, DEST components merge into the JOC structure as appropriate. The JOC structure includes the following standard groups: Command, Operations, Support, and Consequence Management. Representation within the JOC includes some Federal, State, and local agencies.

Lead Agency: The FBI defines lead agency, as used in PDD-39, as the Federal department or agency assigned lead responsibility to manage and coordinate a specific function — either crisis management or consequence management. Lead agencies are designated on the basis of their having the most authorities, resources, capabilities, or expertise relative to accomplishment of the specific function. Lead agencies support the overall Lead Federal Agency during all phases of the terrorism response.

Lead Federal Agency: Several of these plans designate a Lead Federal Agency (LFA) to coordinate the Federal response. The LFA is determined by the type of emergency. In general, an LFA establishes operational structures and procedures to assemble and work with agencies providing direct support to the LFA in order to obtain an initial assessment of the situation, develop an action plan, and monitor and update operational priorities. The LFA ensures that each agency exercises its concurrent and distinct authorities and supports the LFA in carrying out relevant policy. Specific responsibilities of an LFA vary according to the agency s unique statutory authorities.

Logistics Information Management System (LIMS): FEMA s official automated personal property management system.

Long-Range Management Plan: Used by the FCO and team management in a large-scale disaster to address internal staffing and disaster organization and team requirements.

Major Disaster: As defined under the Stafford Act, any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Memorandum of Agreement (MOA): Tripartite written agreement between FEMA, the sponsoring organization for the US&R task force of the National US&R Response System, and the State of the sponsoring organization. The MOA outlines responsibilities of each signatory in the event of an activation of the National US&R Response System. The MOA serves as the basis for reimbursement of task force operational expenditures during activation.

Mitigation: Those activities designed to alleviate the effects of a major disaster or emergency or long-term activities to minimize the potentially adverse effects of future disaster in affected areas.

Mobilization Center: A temporary facility at which emergency services personnel and equipment are temporarily located pending assignment, release, or reassignment. A Base Support Installation may serve as a mobilization center. The designated location at which response personnel and resources are received from the Point of Arrival and pre-positioned for deployment to a local staging area or directly to an incident site as required. A mobilization center also provides temporary support services, such as food and billeting, for response personnel prior to their deployment.

Monitoring Period: The period preceding an incident characterized by assessment and preparatory activities leading to either response activity or stand-down. During this period, the Assessment and Analysis Branch, Operations and Planning Division, FEMA Response and Recovery Directorate, monitors causative factors and phenomena, keeps in close contact with the affected FEMA region(s) and appropriate Federal agencies, and may call for remote sensing data or other assessment actions.

Movement Coordination Center (MCC): An element under ESF #1 that is located at FEMA Headquarters and, if necessary, in the field to coordinate the acquisition of transportation capacity and maintain visibility over validated transportation requests for assistance from inception through delivery to a mobilization center

National Disaster Medical System (NDMS): The National Disaster Medical System (NDMS), a nationwide medical mutual aid network between the Federal and non-Federal sectors that includes medical response, patient evacuation, and definitive medical care. At the Federal level, it is a partnership between HHS, the Department of Defense (DOD), the Department of Veterans Affairs (VA), and the Federal Emergency Management Agency (FEMA).

National Fire Suppression Liaison Officer: The Disaster and Emergency Operations Specialist, Fire and Aviation Management, Forest Service. This person is a member of the EST operating at the national level. Primary responsibility is to provide liaison among the EST, the National Director of Fire and Aviation Management, Forest Service Headquarters, and other support agencies.

National Interagency Coordination Center (NICC): The organization responsible for coordination of national emergency response for wildland fire suppression, located at the National Interagency Fire Center in Boise, ID.

National Oil and Hazardous Substances Pollution Contingency Plan (NCP): The NCP (40 CFR 300) administers the response powers and capabilities authorized by CERCLA and section 311 of the Clean Water Act. The NCP applies to all Federal agencies and provides for efficient, coordinated, and effective response to discharges of oil and releases of hazardous substances, pollutants, and contaminants.

National Response Center (NRC): A national communications center for activities related to oil and hazardous substance response actions. The National Response Center, located at USCG Headquarters in Washington, DC, receives and relays notices of oil and hazardous substances releases to the appropriate Federal OSC. The 24-hour number is 1 (800) 424-8802, or in Washington, DC, (202) 267-2675.

National Response Team (NRT): The NRT, composed of the 16 Federal agencies with major environmental and public health responsibilities, is the primary vehicle for coordinating Federal agency activities under the NCP. The NRT carries out national planning and response coordination and is the head of a highly organized Federal oil and hazardous substance emergency response network. EPA serves as the NRT Chair (Director, Chemical Emergency Preparedness and Prevention Office), and the USCG serves as Vice-Chair.

National Security Council (NSC): FBI requirements for assistance from other Federal agencies will be coordinated through the Attorney General and the President, with coordination of National Security Council (NSC) groups as warranted.

National Strike Force: The National Strike Force consists of three Strike Teams established by the USCG on the Pacific, Atlantic, and Gulf coasts. The Strike Teams can provide advice and technical assistance for oil and hazardous substances removal, communications support, special equipment, and services.

National Voluntary Organizations Active in Disaster (NVOAD): NVOAD is the umbrella organization of established and experienced voluntary organizations that provide disaster services in all phases of emergency management. NVOAD fosters cooperation, communication, coordination, and collaboration among voluntary organizations. It also encourages close working partnerships among voluntary organizations and government at all levels. It is not operational as an organization.

Nuclear Weapons : The Effects of Nuclear Weapons (DOE, 1977) defines nuclear weapons as weapons that release nuclear energy in an explosive manner as the result of nuclear chain reactions involving fission and/or fusion of atomic nuclei.

On-Scene Coordinator (OSC): The Federal official pre-designated to coordinate and direct hazardous substance removal actions. Depending upon the location of the incident, the OSC may be provided either by EPA, USCG, DOD, or DOE. OSCs from DOD and DOE will be used to coordinate and direct actions at their respective agency facilities.

Operating Site: The location of a structural collapse where US&R operations are being conducted.

Operational Period: The period of time scheduled for completion of a given set of operations actions as specified in the action plan, usually 24 hours. This period usually defines the reporting period for SITREPs and plans that address operational priorities.

Personal Property: Any property other than real property, which includes land, buildings, and other structures owned or leased by the Federal Government. In this annex, personal property is used interchangeably with goods, equipment, and supplies.

Point of Arrival (POA). The designated location (typically an airport) within or near the disaster-affected area where newly arriving staff, supplies, and equipment are initially directed. Upon arrival, personnel and other resources are dispatched to either the DFO, a mobilization center, a staging area, or directly to a disaster site. (See Aerial Port of Debarkation.)

Point of Departure (POD). The designated location (typically an airport) outside the disaster-affected area from which response personnel and resources will deploy to the disaster area. (See Aerial Port of Embarkation.)

Preliminary Damage Assessment (PDA): Under the Stafford Act, a Governor may request the President to declare a major disaster or an emergency if an event is beyond the combined response capabilities of the State and affected local governments. Based upon the findings of a joint Federal-State-local Preliminary Damage Assessment (PDA) indicating the damages are of sufficient severity and magnitude to warrant assistance under the Act, the President may grant a major disaster or emergency declaration. (Note: In a particularly fast-moving or clearly devastating disaster, the PDA process may be deferred until after the declaration.)

Presidential Decision Directive 39 (PDD-39): Presidential Decision Directive 39 (PDD-39), U.S. Policy on Counterterrorism, establishes policy to reduce the Nation s vulnerability to terrorism, deter and respond to terrorism, and strengthen capabilities to detect, prevent, defeat, and manage the consequences of terrorist use of weapons of mass destruction (WMD). PDD-39 states that the United States will have the ability to respond rapidly and decisively to terrorism directed against Americans wherever it occurs, arrest or defeat the perpetrators using all appropriate instruments against the sponsoring organizations and governments, and provide recovery relief to victims, as permitted by law.

Primary Agency: **(a)** Each ESF is headed by a primary agency designated on the basis of its authorities, resources, and capabilities in the particular functional area. Other agencies have been designated as support agencies for one or more ESFs based on their resources and capabilities to support the functional area(s). **(b)** A Federal agency designated as an ESF primary agency serves as a Federal executive agent under the FCO to accomplish the ESF mission. When an ESF is activated in response to a disaster, the primary agency for the ESF has operational responsibility for:

1. Orchestrating the Federal agency support within the functional area for an affected State;
2. Providing an appropriate level of staffing for operations at FEMA Headquarters, the ROC, DFO, and DRC;
3. Activating and subtasking support agencies;
4. Managing mission assignments and coordinating tasks with support agencies, as well as appropriate State agencies;
5. Supporting and keeping other ESFs and organizational elements informed of ESF oper ational priorities and activities;
6. Executing contracts and procuring goods and services as needed;
7. Ensuring financial and property accountability for ESF activities; and
8. Supporting planning for short- and long-term disaster operations.

Radiological Emergency Response Teams: EPA s Office of Indoor Air and Radiation provides Radiological Emergency Response Teams (RERTs) to support and respond to incidents or sites containing radiological hazards. These teams provide expertise in radiation monitoring, radionuclide analyses, radiation health physics, and risk assessment. RERTs can provide both mobile and fixed laboratory support during a response.

Reconstruction Information Center (RIC): A center dealing only with mitigation in reconstruction and rebuilding techniques may be called a Reconstruction Information Center (RIC). A RIC may be set up at a fixed or mobile location.

Recovery: Activities traditionally associated with providing Federal supplemental disaster relief assistance under a Presidential major disaster declaration. These activities usually begin within days after the event and continue after response activity ceases. Recovery includes individual and public assistance programs that provide temporary housing assistance, as well as grants and loans to eligible individuals and government entities to recover from the effects of a disaster.

Regional Emergency Coordinator (REC): The GSA REC or a designated alternate is the regional point of contact for FEMA alerts and requests for assistance.

Regional Emergency Transportation Coordinator (RETCO): In the disaster area, direction of the ESF #1 mission is provided by the DOT Regional Emergency Transportation Coordinator (RETCO). The RETCO is the Secretary of Transportation s representative for emergency preparedness and response matters and is the senior regional ESF #1 official for both planning and execution.

Regional Operations Center: The Regional Operations Center (ROC) staff coordinates Federal response efforts until an ERT is established in the field and the FCO assumes coordination responsibilities. Generally operating from the FEMA Regional Office, the ROC establishes communications with the affected State emergency management agency and the EST; coordinates deployment of the Emergency Response Team Advance Element (ERT-A) to field locations; assesses damage information and develops situation reports; and issues initial mission assignments. The ROC is activated by the FEMA Regional Director based on the level of response required. It is led by a ROC Director and consists of FEMA staff and ESF representatives, as well as a Regional Emergency Preparedness Liaison Officer (REPLO) who assists in coordination of requests for military support. Financial management activity at the ROC will be monitored and reported by the Comptroller.

Regional Response Teams (RRTs): Regional counterparts to the NRT, the RRTs are made up of regional representatives of the Federal agencies on the NRT and representatives of each State within the region. The RRTs serve as planning and preparedness bodies before a response, and provide coordination and advice to the Federal OSC during response actions.

Regional/Area Fire Coordinator: The person primarily responsible for operation of ESF #4 at the regional level.

Requirements Processing: Analysis of requests for goods or technical services, translating these requests into meaningful specifications, completing requisite paperwork (e.g., Request for Federal Assistance form or FEMA Form 40-1), and entering the request into the resource tracking system. Alternately known as the resource ordering process.

Resource Tracking: Monitoring the processing of requirements, source selection, movement, receipt, distribution, utilization, and recovery of goods, tactical teams, and technical service personnel for a specific operation. The resource tracking function is a subcomponent of FEMA s overall asset visibility system since it focuses only on the movement of a small group of items,

teams, and personnel from the Federal Government s resources.
Resources: All personnel and major goods available, or potentially available, for assignment to operations. Resources are described by kind and type.
Response: Activities to address the immediate and short-term effects of an emergency or disaster. Response includes immediate actions to save lives, protect property, and meet basic human needs. Based on the requirements of the situation, response assistance will be provided to an affected State under the FRP using a partial activation of selected ESFs or the full activation of all ESFs to meet the needs of the situation.
Scientific Support Coordinator (SSC): Under the direction of the Federal OSC, a Scientific Support Coordinator leads a team of scientists that provides scientific support for response operational decisions and for coordinating on-scene scientific activity. Generally, a Scientific Support Coordinator is provided by NOAA in coastal zones and by EPA in the inland zone.
Senior FEMA Official: The official appointed by the Director of FEMA or his representative to represent FEMA on the Command Group at the Joint Operations Center. The Senior FEMA Official is not the Federal Coordinating Officer.
Situation Assessment: The evaluation and interpretation of information gathered from a variety of sources including weather information and forecasts, computerized models, GIS data mapping, remote sensing sources, ground surveys, etc. that, when communicated to emergency managers and decision makers, can provide a basis for response and recovery decision making.
Situation Reports (SITREPs): Periodic summaries of the disaster situation, including the status of operations, geographical information, identification of operational priorities and requirements, reports from specific ESFs on their major response and recovery activities, unmet needs, and recommended actions, as well as data on human services, infrastructure, and mitigation programs.
Situation Room: An area in the State EOC, ROC, DFO, or FEMA Headquarters used for the display of iStaging Area.
State Coordinating Officer (SCO): The FCO works closely with the State Coordinating Officer (SCO), appointed by the Governor to oversee disaster operations for the State, and the Governor s Authorized Representative (GAR), empowered by the Governor to execute all necessary documents for disaster assistance on behalf of the State.
Status Briefing: A briefing by ERT or EST personnel that summarizes the current situation, operational priorities, and the status of Federal response operations in support of a disaster.
Strategic Information and Operations Center (SIOC): If warranted, the FBI implements an FBI response and simultaneously advises the Attorney General, who notifies the President and NSC groups as warranted, that a Federal crisis management response is required. If authorized, the FBI activates multiagency crisis management structures at FBI Headquarters, the responsible FBI Field Office, and the incident scene. Federal agencies requested by the FBI, including FEMA, will deploy a representative(s) to the FBI Headquarters Strategic Information and Operations Center (SIOC) and take other actions as necessary and appropriate to support crisis management. (The FBI provides guidance on the crisis management response in the FBI WMD Incident Contingency Plan.)
Strategic Plan: Addresses long-term issues such as impact of weather forecasts, time-phased resource requirements, and problems such as permanent housing for displaced disaster victims, environmental pollution, and infrastructure restoration.
Supervisor of Salvage and Diving (SUPSALV): SUPSALV is a salvage, search, and recovery

operation established by the Department of Navy. SUPSALV has extensive experience to support response activities, including specialized salvage, firefighting, and petroleum, oil, and lubricants offloading. SUPSALV, when available, will provide equipment for training exercises to support national and regional contingency planning.

Support Agency: **(a)** Each ESF is headed by a primary agency designated on the basis of its authorities, resources, and capabilities in the particular functional area. Other agencies have been designated as support agencies for one or more ESFs based on their resources and capabilities to support the functional area(s). **(b)** When an ESF is activated in response to a disaster, each support agency for the ESF has operational responsibility for:

1. Supporting the ESF primary agency when requested by conducting operations using its authorities, cognizant expertise, capabilities, or resources;
2. Supporting the primary agency mission assignments;
3. Providing status and resource information to the primary agency;
4. Following established financial and property accountability procedures; and
5. Supporting planning for short- and long-term disaster operations.

System to Locate Survivors (STOLS): An acoustic listening device used by specially trained personnel from the U.S. Army Corps of Engineers for the location of victims trapped in collapsed structures.

Technical Assistance: Is provided to State and local jurisdictions when they have the resources but lack the knowledge and skills needed to perform a required activity (such as mobile-home park design and hazardous material assessments).

Technical Operations: As used in this annex, technical operations include actions to identify, assess, dismantle, transfer, dispose of, or decontaminate personnel and property exposed to explosive ordnance or WMD.

Territory Logistics Centers (TLCs): FEMA s strategically located logistics centers that support disaster operations through a variety of preparedness and response measures. These centers serve as storage sites for strategic disaster supplies and equipment, including initial supplies of certain IRR goods and prepackaged kits to support disaster field facilities. Skilled logistics personnel may be supplied from these centers to support disaster operations. Three geographically dispersed TLCs are located at Fort Gillem, GA; Fort Worth, TX; and Moffett Field, CA.

Terrorist Incident: The FBI defines a terrorist incident as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

Time-Phased Force and Deployment List (TPFDL): A tool to manage the rapid, systematic movement of Federal response personnel, equipment, and critical relief supplies into an affected area in accordance with operational priorities

Unaffiliated Volunteer: Also known as a "spontaneous" or "emergent" volunteer; an individual who is not formally associated with a recognized voluntary disaster relief organization.

Undesignated Goods: Largely unsolicited, donated items that are not addressed to a specific recipient.

Unsolicited Goods: Donated items that have not been requested by government officials, voluntary disaster relief organizations, or other donations-related personnel.

Voluntary Organizations Active in Disaster (VOAD): VOAD is a coalition of voluntary organizations organized at State and local levels. In nondisaster periods, it meets to discuss emergency management issues and encourage cooperation, communication, coordination, and collaboration among voluntary organizations. In the response period, each individual organization functions independently, yet cooperatively.

Weapon of Mass Destruction (WMD): Title 18, U.S.C. 2332a, defines a weapon of mass destruction as (1) any destructive device as defined in section 921 of this title, [which reads] any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one-quarter ounce, mine or device similar to the above; (2) poison gas; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Recommending Reading

1.) Alibek, Ken, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World, Told from the Inside by the Man Who Ran it*, New York, Random House, 1999.
2.) Center for Disease Control and Prevention, *Preventing Emerging Infectious Diseases, A Strategy for the 21st Century*; Atlanta, GA, U.S. Department of Health and Human Services, 1998.
3.) Center for Disease Control and Prevention, *Emerging Infectious Diseases: Tracking Trends and Analyzing New and Reemerging Infectious Disease Issues Around the World*, Department of Health and Human Services, Vol. 5, No.4, July-August 1999.
4.) Congressional Research Service Library of Congress, *International Terrorism: A Compilation of Major Laws, Treaties, Agreements, and Executive Documents*, Washington, DC, 2000.
5.) Coogan, Tim Pat; *Michael Collins: A Biography, London*, Hutchinson, 1990.
6.) Cordesman, Anthony H., *Weapons of Mass Destruction in the Middle East, London*, Brassey s, 1991.
7.) Dando, Malcolm, *Biological Warfare in the 21st Century : Biotechnology and the Proliferation of Biological Weapons*.
8.) Deighton, Len, *Bomber;Events Relating to the Last Flight of an R.A.F. [bomber] over Germany on the Night of June 31, 1943*, New York, Harper & Row,1970.
9.) Department of Defense, *The Militarily Critical Technologies List; Part II Weapons of Mass Destruction Technologies*, Washington, DC, Office of the Under Secretary of Defense for Acquisition and Technology,1998.
10.) Falkenrath, Richard A.; Newman,Robert D.; Thayer, Bradley A, *America s Achilles Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*, Cambridge, MA, The MIT Press, 1998.
11.) Fraser, Antonia, *Faith and Treason : The Story of the Gunpowder Plot*, New York, Doubleday,1996.
12.) Fraser, Antonia, *The Gunpowder Plot : Terror & Faith in 1605*, London, Weidenfeld & Nicolson,1996.
13.) Garrett, Laurie, *The Coming Plague: Newly Emerging Diseases in a World Out of Balance / Laurie Garrett*, New York, Penguin Books, 1994.
14.) Garrett, Laurie, *Microbes Versus Mankind : The Coming Plague*, New York, Foreign Policy Association,1996.
15.) Henderson, Donald A.; Inglesby, Thomas V.; Bartlett, John G. et al., *Smallpox as a Biological Weapon: Medical and Public Health Management*, JAMA.1999;281:2127-2137.
16.) Hoffman, Bruce, *Inside Terrorism*, New York, Columbia University Press,1998.
17.) Inglesby, Thomas V.; Dennis,David T.; Henderson, Donald A.. et al. *Plague as a Biological Weapon*, *Medical and Public Health Management*, JAMA. 2000;283:2281-2290.

18.) Inglesby, Thomas V.; Henderson,Donald A.; Bartlett, John G. et al*., Anthrax as a Biological Weapon*, *Medical and Public Health Management*, JAMA,1999;281:1735-1745.

19.) Institute for Security Technology Studies at Dartmouth College, *Emerging Threats Assessment*, Home Page, http://thayer.dartmouth.edu/~ethreats/.

20.) Jeremiah, USN (Ret), Admiral David E., *Nanotechnology and Global Security*, http://www.zyvex.com/nanotech/nano4/jeremiahPaper.html.

21.) Kaplan, David E.; Marshall, Andrew, *Cult at the End of the World; The Terrifying Story of Aum Doomsday Cult, from the Subways of Tokyo to the Nuclear Arsenals of Russ*, Crown Publishers Inc., 1996.

22.) Karlen, Arno, *Man and Microbes : Disease and Plagues in History and Modern Times*, Touchstone Books, 1996.

23.) Lanciotti, R. S.; Roehrig,J. T.; Deubel, V. et al, *Origin of the West Nile Virus Responsible for an Outbreak of Encephalitis in the Northeastern United States*, Science, 1999;2333-2337.

24.) Lederberg, Joshua, ed. *Biological Weapons: Limiting the Threat*, Cambridge, MA, MIT Press, 1999.

25.) Libicki, Martin,*The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, Washington, DC, National Defense University,1995.

26.) Macintyre, Anthony G.; Christopher,Lt COL George W.; Eitzen, COL Edward et al.,*Weapons of Mass Destruction Events With Contaminated Casualties*, *Effective Planning for Health Care Facilities*, JAMA.2000;283:242-249.

27.) Murray, Williamson; Knox, MacGregor; Bernstein, Alvin. eds., *The Making of Strategy: Rulers, States and War*, Cambridge, Eng, Press Syndicate of the University of Cambridge,1994.

28.) National Research Council, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response*,Washington, DC, National Academy Press, 1999.

29.) New York City Mayor s Office of Emergency Management and Departments of Fire, Health, Environmental Protection and Police, *Biological Warfare Improved Response Program: 1998 Summary Report on BW Response Template and Response Improvements*, 1999.

30.) Office of Technology Assessment,*Technologies Underlying Weapons of Mass Destruction*, Washington, DC, U.S. G.P.O.,1993.

31.) Perl, Raphael F.,*CRS Report for Congress 97-960 F, Terrorism, the Media, and the Government: Perspectives, Trends, and Options for Policymakers*,Washington, DC, Congressional Research Service, The Library of Congress,1997.

32.) Perl, Raphael F.; O Rourke,Ronald, *CRS Report for Congress RS20721, Terrorist Attack on USS Cole: Background and Issues for Congress*, Washington, DC, Congressional Research Service, The Library of Congress,2000.

33.) Perl, Raphael F., *CRS Report for Congress 98-733 F, Terrorism: U.S. Response to Bombings in Kenya and Tanzania: A New Policy Direction?,* Washington, DC, Congressional Research Service, The Library of Congress,1998.

34.) Preston, Richard, *The Hot Zone*, New York, Random House, 1994.

35.) RAND, *First Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*,Washington, DC, RAND,1999.
36.) RAND, *Second Annual Report Toward a National Strategy for Combating Terrorism*, www.rand.org/organization/nsrd/terrpanel, December 14, 2000.
37.) Roberts, Brad*, Hype or Reality: The New Terrorism and Mass Casualty Attacks*, Alexandria, VA, The Chemical and Biological Arms Control Institute,2000.
38.) Scheld, W. Michael; Craig,William A.; Hughes, James M.. eds*., Emerging Infections 3*, Washington, DC, ASM Press,1999.
39.) Schwabe, William, *Needs and Prospects for The Federal Role in Assisting State and Local Law Enforcement*, Washington, DC, RAND1999.
40.) Senate Armed Services Committee Hearings*, Global Proliferation of Weapons of Mass Destruction*,1996 .
41.) Sidell, MD, Frederick R.; Takafuji, MD, MPH,Ernest T.; Franz, DVM,PhD, David R.. eds., *Medical Aspects of Chemical and Biological Warfare*, Washington, DC, Office of The Surgeon General, Department of the Army, United States of America.
42.) Smithson, Amy E.; Levy,Leslie-Anne; *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*, Washington, DC, The Henry L. Stimson Center,1999.
43.) Stern, Jessica, *The Ultimate Terrorists*, Cambridge, MA, Harvard University Press,1999.
Naval Studies Board*, Technology for the United States Navy and the Marine Corps, 2005-2035: Becoming a 21st-Century Force*, Washington, DC, National Academy Press, 1997.
44.) Tucker, Jonathan B., ed.,*Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge, MA, MIT Press, 2000.
45.) United States Army Medical Research Institute of Infectious Diseases*, Medical Management of Biological Casualties Handbook, 3rd e*d., Frederick, Md., United States Army Medical Research Institute of Infectious Diseases, 1998.
46.) United States Department of State, *Patterns of Global Terrorism 1999*, Washington, DC, 2000.
47.) United States. Congress. Senate. Committee on Governmental Affairs. Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction : Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, One Hundred Fourth Congress, first session*, 1996.
48.) United States. Congress. Senate. Committee on Governmental Affairs. Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction : Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, One Hundred Fourth Congress, first session*.
49.) United States. Congress. Senate. Committee on Governmental Affairs. Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction : Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, One Hundred Fourth Congress, first session,* Washington, DC, U.S. G.P.O., 1996.

Summary and Status of Web Site
Institute for Security Technology Studies: Emerging Threats Assessment

Ann Marion

Background:

Dartmouth College launched a new program in 2000 focusing on cyber-security and information infrastructure protection research. The Institute for Security Technology Studies serves as a principal national center for counter-terrorism technology research, development and assessment. It is funded by the U.S. Justice Department's National Institute of Justice, Office of Science and Technology to which it will also provide technical support. An Informational Web Site, publicly accessible, was established.

A new section of the Institute Web Site was developed for Emerging Threats Assessment. The mission of this section of the ISTS Web Site is to support a series of meetings and consortia. As the meetings draw on expertise outside as well as inside of Dartmouth, the web site is intended to provide a mechanism for coordination and information sharing, before, during, and after, the meeting sessions. The meetings themselves are face to face, but communication before, and after, will be facilitated through the web site, email, and other means.

A goal of this section of the Institute web site is to achieve a high level of efficiency and economy, particularly over the first 3-6 months. However, as the Institute matures in it s vision, increasingly sophisticated mechanisms and technologies will be required to sustain it. An objective of the information architecture process will be to define evolution of the site, exploring alternatives for scalability, security, content management, and administration. These may not be necessary at the outset, but a plan for transition will inform the design.

Deliverables:

The Web Site proved an excellent publishing medium that facilitated the collection of documents from a diverse group of participants. Many contributors also provided related links or news items. Downloading documents in a range of formats was implemented in response to requests from participants wanting to read colleagues papers. A flurry of email attests to the use of the Web Site as a document exchange. The web site is maintained on an on-going basis by the web master, Ann Marion, who updates Documents and Verifies links.

<u>Statistics:</u>

- The Web Site Contains 110 HTML Pages, and 115 Downloadable Documents
- There are nearly 2000 links, of which 288 are external to site
- 40 links operative on the Internet Links page
- 9 Bios and 15 White Papers (Reviewed) also have links

<u>PUBLIC Section of the Site:</u>

The Emerging Threats Assessment has branched off of the public ISTS website at Dartmouth.

PASSWORD PROTECTED Section of the Site:
September Working Group (in Progress, Password Required). This section of the site contains work in progress, and is limited to a small circle of participants.

TABLE:
PUBLIC Section of the Site:

Summary	**Agenda**	**Participants**	**White Papers**	**Background**	**Contact**
Summary of July 7-9 Conference •Downloadable files	Agenda for July 7-9 Conference links to: • 15 papers • 7 bios	59 People links to: • 15 papers • 7 bios	15 papers HTML/Text &Word/Word Perfect • RTF formats • Links to Affiliated Institutions	Short Background of Emerging Threats Assessment	Contact information for ISTS and site Web Master

News
Highlights recent publications recommended by participants

Bios
9 Bio Pages • Links to Affiliated Institutions

TABLE: PASSWORD PROTECTED Section of the Site:
September Working Group (in Progress, Password Required)

PASSWORDS:
For this section, you need to be approved as a participant. The purpose of passwords is to provide limited discussion among a working group contributing to the development of draft documents. The Web Master will assign you an individual password, or you can use the group password:

USERNAME: islands
PASSWORD: thousands

Executive Summary	**Franz White Paper**	**Time Frames Feedback**	**2005 Scenario**	**2025 Scenario / Rosen July White Paper**	**List provided by participant**
Short Mission Statement for this Working Group	This is the basis for feedback from the group	In Progress • Outlines	2005 Scenario for a Terrorist Act	Dr. Rosen presented this possible future Sunday morning July	• 40 links updated • 68 orgs.

FIGURE: See Attached File:

Institute for Security Technology Studies at Dartmouth:
Emerging Threats Assessment

HOME PAGE:

http://engineering.dartmouth.edu/~ethreats/

Screen Shot of Introductory Page for Emerging Threats Assessment shows new look implemented in September, 2000.

Navigation Bar is in Left Hand Margin, connecting to all Public Pages, as well as to ISTS.

<u>LIST of URLS for Individual Pages:</u>

Institute for Security Technology Studies at Dartmouth: HOME PAGE
http://www.ists.dartmouth.edu/

Institute for Security Technology Studies at Dartmouth: Emerging Threats Assessment HOME PAGE:
http://engineering.dartmouth.edu/~ethreats/

<u>Conference Summary:</u>
http://engineering.dartmouth.edu/~ethreats/JulyProceedings.html

White Papers:
http://engineering.dartmouth.edu/~ethreats/ethreats6.html

Agenda:
http://engineering.dartmouth.edu/~ethreats/ethreats3.html

Participants:
http://engineering.dartmouth.edu/~ethreats/ethreats4.html

Background:
http://engineering.dartmouth.edu/~ethreats/ethreats7.html

Contact:
http://engineering.dartmouth.edu/~ethreats/ethreats5.html

Working Group: PASSWORD REQUIRED:
http://engineering.dartmouth.edu/~ethreats/2025

Executive Summary:
http://engineering.dartmouth.edu/~ethreats/2025/ExecSummary.html

2005 Scenario:
http://engineering.dartmouth.edu/~ethreats/2025/Scenario.html

2025 Scenario:
http://engineering.dartmouth.edu/~ethreats/2025/whitepapers/2025Scenario.html

TimeFrames/Recommendations:
http://engineering.dartmouth.edu/~ethreats/2025/recommendations/Rec1.html

Franz White Paper:
http://engineering.dartmouth.edu/~ethreats/whitepapers/FRANZ/FranzHTML/Epi%20of%20BT%20Franz.2.htm

News:
http://engineering.dartmouth.edu/~ethreats/whitepapers/News.html

Internet Links:
http://engineering.dartmouth.edu/~ethreats/2025/whitepapers/Links.html

FIGURE: NAVIGATION SEE ATTACHED FILE

On the Left:
Navigation for
~ethreats Home Page
[Public Site]

On the Right:
Navigation for
~ethreats/2025 Home Page
[PASSWORD PROTECTED Site]

PUBLIC SITE

PASSWORD PROTECTED

Summary of Conference Papers[1]

Prepared by
Charles Lucey, MD, JD, MPH

Introduction

The following papers were submitted for the July, 2000 conference, "Emerging Threats Assessment — Biological Terrorism: A Technology-Based Threat Assessment." As indicated previously, the project process included an additional key workshop in September designed to refine and carry forward the work set out in July. This Executive Summary distills the essence of each submitted paper (while avoiding overlap with other papers, when possible) and, in some cases, includes the Editor's commentary to provide additional context. These papers are published in a separate publication to be entitled, "Emerging Threats Assessment: Biological Terrorism 2000 to 2025." This may also be found on line at www.thayer.dartmouth.edu/~ethreats/. Together with the Section summarizing the actual conference discussions, this Section provides a background within which to understand the Emerging Threats 2000-2025's Findings and Conclusions.

Project Papers

"Challenges in Coordinating the Response to Bioterrorism," Mike Ascher, MD

In "Challenges in Coordinating the Response to Bioterrorism," Mike Ascher, MD, Chief, Viral and Rickettsial Disease Laboratory Branch, Berkely, CA, writes that the overall impact of a terrorist attack will be determined by the ability of the public health system to respond to the threat organism. Key components of public health system are disease detection, organism identification, antibiotic therapy or immunization, and environmental mitigation. Dr. Asher believes that the myriad components of the response system are poorly organized currently.

Dr. Ascher cites the recent National Commission on Terrorism report to support his view that federal leadership must better coordinate funding, response planning, eliminating coverage gaps, and avoid duplication. A second area of concern is that biological response planning has been treated as a variant of chemical response training. Dr. Asher is also concerned that the National Guard no longer has the resources necessary to respond to an emergency situation. While being given a prominent role in response planning, it lacks hospitals or medical personnel to properly treat victims. He concludes that there are major challenges in coordinating necessary

---

1 Summary of submitted papers in alphabetical order by author. These views expressed represent the private views of the author, unless explicitly stated in the referenced paper.

resources to respond to a bioterrorist event. It is essential to establish a new and on-going planning process that engages all parties, particularly public health, likely to be the first responders. He believes it is necessary to rethink disaster response from the pragmatic perspective of first responders in a biological event. Such planning is dual-use, required for responding to any disaster or epidemic, whether naturally occurring or from a hostile attack.

"Examining the Military and Law Enforcement Terrorism Counteraction Model: A Template for Medical Response to Biological Terrorism?" William L. Bograkos, DO, FACOEP and Daniel J. Kaszeta

William Bograkos, DO, and Daniel Kaszeta are members of the Maryland National Guard who presented a white paper on their template for biological terrorism response. Their paper defines terrorism employing the FBI definition which is "a violent act or an act dangerous to human life, in violation of the criminal laws of the United States or of any state, to intimidate or coerce the government, civilian population, or any segment thereof in furtherance of political or social objectives." They believe that their template will be useful to both the medical and the law-enforcement communities. Using a counterterrorism model that the United States Army developed in 1984, the authors formulate a step model adapted to the medical/first responder community.

Step one of the template is medical intelligence, which includes medical surveillance. This will primarily be the responsibility of public health official epidemiologists. This surveillance must look for unusual occurrences that must be separated from background events. The Centers for Disease Control does have the Epidemiology and Laboratory Capacity program, and the Emerging Infectious Programs to contribute to this effort. Medical intelligence also includes agent identification. This may require animal study, mass spectroscopy, immunoassay, DNA probes, and other advanced techniques.

Step two requires a threat analysis that is ongoing and active. This requires continuing to educate the providers on agent awareness and characteristics of agent attack. Awareness also requires ongoing analysis of infrastructure, and planning for vulnerability to new attack scenarios. It also requires ongoing communication with other planners and agencies. In addition, threat analysis requires credibility assessment, and prioritizing threats which may be organized along scientific, operational, and psychological analysis. Hoaxes must be differentiated from real threats.

Steps three through five are the antiterrorism measures of physical security, personal security, and operational security. Physical security involves the maintaining of hospital security/crowd control, decontamination, and physical infrastructures, such as air intakes.[2]

---

[2] Dr. Richard Hutchinson also points out, in his paper, that securing and purifying air circulation might be cost-effective for public spaces.

Personal security includes such matters as protective equipment, universal precautions, immunization, and chemoprophylaxis.[3] Operational, defensive security includes such issues as coordination, preserving safety of water supplies and transportation systems, and maintaining supplies, including medical and logistical.

The authors identify step 6, information security, as its own step, promoting it from its listing as a subdiscipline of operational security in the original 1984 model. The authors do this based on the fact that information technology has become so important with the ubiquitous automation of hospitals, medical systems, and emergency response systems. Bograkos and Kaszeta point out that information warfare can multiply the effects of biological attack by contributing greatly to the chaos. Information warfare/terrorism could interfere with horizontal communications, vertical communications, technical information references, clinical testing and diagnostics, and the actual power grids themselves.

Step 7 is authority and jurisdiction. This refers to maintaining law and order, and possibly includes the use of quarantine authority. This would include forensics, and the need to respect international law and treaties. In step 8, the authors list all of the elements of crisis/consequence management and planning. They provide a 20-step guideline to show how this might be organized, and suggest that training and practice are key for performance. The authors discuss possible threats both from criminals and the criminally insane. Bograkos and Kaszeta believe that good preparation for Bioterrorism will be protective against these other forms of violence. They stated that they worry as much about the psychology of terrorists who would desire to acquire and use such weapons do about the use of biological agents.

"Information Technology and the Medical Response to Bioterrorism," Jon Bowersox, MD, PhD

Dr. Bowersox, Division of Vascular Surgery, University of California, San Francisco, overviews the recent history of health information technology, noting that health care has invested in this at half of the rate of industries such as transportation and financial services. Jon writes that telemedicine is used by less than 1% of health care providers on a regular basis but predicts that broadband communications and dropping costs will make its use increasingly common. He predicts that handheld, mobile devices will be increasingly used for remote physiological monitoring, point-of-care laboratory testing, clinical record keeping, and telemedicine, with voice recognition software eliminating the need for keyboards.

Dr. Bowersox reviews the CDC efforts to create a Health Alert Network (HAN). This will be an Internet system to link local health officials into an integrated nationwide system for epidemiological investigation, training, and rapid communication. The National Electronic Disease Surveillance System (NEDSS) is being developed to integrate many disease surveillance systems currently being used and to incorporate new data analysis tools. The Common Interface for Public Health Electronic Reporting (CIPHER) is establishing standards for data elements record

[3] As Dr. Franz points out, these may be more practical for military personnel and civilian person

ing for laboratories to report on-line. "BTTv" is a CDC service to educate using video streaming for bioterrorism preparedness and response.

The World Health Organization (WHO) is developing Internet surveillance, as are other organizations and universities. Jon states that the challenge for public health informatics developers is to extend the reach of data acquisition and knowledge dissemination. He believes that by integrating real time data of billing diagnostic codes, pharmacy, over the counter (OTC) remedies, etc., we can use historical comparisons to detect new epidemics or terrorist attack. Dr. Bowersox relies on the Health Insurance Portability and Accountability Act of 1996 to set stringent standards for ensuring patient confidentiality. Electronic medical records will use negotiated industry standards for sharing data combined with XML software coding to allow tremendous data mining.

"The Infrastructure Web: A System for Distributed Monitoring and Management," George Cybenko, PhD, and Guofei Jiang, PhD

George Cybenko, PhD, Dartmouth College, and Guofei Jiang, PhD, ISTS describe their system for distributed monitoring and management of critical national infrastructures, employing a web-like architecture. Historically, one should remember that the Web began as a DARPA project to distribute the computer servers and message routing so that nuclear attack could not interrupt the flow of critical information.

Critical infrastructure protection depends on many processes: intelligence gathering, analysis, interdiction, detection, response and recovery, etc. They must be applied both to complicated individual systems and to the increasingly interdependent and complex couplings. This interaction can involve telecommunications, the Internet, utilities, law-enforcement, emergency management, and commerce. Cybenko and Jiang worry that these threats are evolving at "Internet time," speedily mutating and attacking. They propose a system to use sensors, and other tools to protect our infrastructure. The sensors may be mechanical, or may be software programs that monitor communication or information systems for example.

"The New Battlefield in our City Streets: The Epidemiology of Biological Terrorism in the US and Some Thoughts on the Way Ahead," David Franz, PhD

Dr. David Franz, Southern Research Institute, reviewed the modern history of biological warfare and gave his opinion on program priorities in his white paper. Dr. Franz points out that Russia continued the most impressive program in the history of humankind 20 years after ratifying the Biological Weapons Convention of 1972. With the history and experience of the Gulf War, it has become evident that there is a potential biological terrorism threat to our cities. Unfortunately, treaties have little impact on terrorism and the dual-use nature of bioweapons production can make treaty verification very difficult. We do not understand the limits of biology -- for good or for evil. We must therefore be capable of responding quickly and effectively to the unknown.

This requires a deep technological base from which to respond. We must leverage existing programs, partners, and the pharmaceutical industry for advanced development of orphan vaccines and antiviral drugs. Second, intelligence gathering for Bioterrorism is difficult because of the minimal signature of terrorist weapons programs. Dr. Franz suggests that we use data mining and other information technologies to improve our intelligence gathering capabilities and build our intelligence capabilities over the long term.

The third research priority is forensics. We must be able to quickly dissect the organism at the molecular level. Genetic fingerprinting will be useful in world courts of law. Fourth, there must be a will to retaliate using an approach that is vigilant, integrated, uncompromising, and swift. The clear understanding of our resolve will be a deterrent. A fifth priority is medical counter measures. These range from basic research on the immune system, to vaccine and drug development, to improving diagnostic tools. We must improve our stockpiling efforts in preparation for attack. We must prepare for the rapid acquisition of necessary equipment, hospital bed space, ventilators and other supplies. Preparation must also include planning for psychological counseling.

Priority 6 is physical countermeasures. Presently, sensor technologies for biological terrorism are not widely employable. Dr. Franz believes that modification of HVAC systems in critical public buildings may have utility for collective protection. Without timely warning, protective masks have little utility. The seventh priority is to strengthen the public health infrastructure. This involves effective surveillance, improved laboratory capabilities, epidemiology, teaching, and public health practice. Investment in public health is particularly cost-effective. Issue number eight is improving interagency collaboration. This must be done vertically, from the local to national level and horizontally, across different agencies and responders. Exceptional leadership will facilitate this collaboration.

The ninth priority is educational programs. Many of the diseases that may be used in a biological attack are unfamiliar to our public health care providers. Training, planning, and drills must prepare physicians and staff for mass-casualty patient management Engineers and hospital administrators must be familiar with technical biological containment issues so they can improvise containment for patient rooms, etc. Tenth, we must exploit the phenomenal advances in biotechnology, telemedicine, robotics, virtual reality, simulation, nanotechnology, Internet, and wireless communications. Finally, the concept of complementary programs includes areas such as improving law and treaty enforcement, international justice, expanding cooperative threat reduction programs where possible, and redoubling our efforts to eliminate biological weapons programs.

"Biological Terrorism Variables and Emergency Response Concepts," Richard Hutchinson, PhD

Dr. Hutchinson, Biological Weapons Improved Response Program Leader, at the U.S. Army to Soldier and Biological Chemical Command, focuses on responding to terrorist use of biological weapons against U.S. population centers. Dr. Hutchinson's paper begins by reviewing some of the key biological variables. Biological agents can be characterized as lethal or non-lethal, treatable or non-treatable, contagious or non-contagious. These different variables require different approaches in planning responses to biological attacks.

Dr. Hutchinson reviews the routes of infection. These are characterized as through inhalation, ingestion, or dermal contact. Aerosol dissemination is still our main worry. Dry powder agent is easiest to release and can have the greatest efficiency for dispersing the agent optimally. Explosive devices, using slurry, have an aerosol efficiency (quantity in atmosphere capable of infecting our lungs) of .1 percent compared to that of 20 percent or higher for dry powder. Liquid spray devices, such as a crop duster, have intermediate efficiency. Besides the means of dispersing the aerosol, it is quite important that the particles be one to five microns in diameter to settle most deeply into victims lungs. For most biological agents, the attack residual, which settles after primary attack, poses little threat to the general population, but may threaten rescue workers and others in intimate contact.

Dr. Hutchinson makes the point that response plans have to be able to respond to a wide range of casualties, depending upon the particular organism and means of dispersal. Dr. Hutchinson's team has studied different scenarios in an effort to formulate a response template that can be programmed for different communities to use. He states that detection and diagnosis of the disease is likely to occur 3 to 4 days after attack. Using anthrax as an example, he estimates that casualties seeking medical care would peak around five to six days after the attack and that 10 times the number of casualties would seek help as "the worried well." The unpredictable scale of biological attacks means that communities will have to plan for outside resources to back-up local medical care. His group s scenario analysis reinforces the need for prevention and preparation. The impact could be devastating, even if the overall threat has a low likelihood. A response strategy must therefore balance the daunting challenge of preparation with the cost, effort, and difficulty of implementation.

Dr. Hutchinson presents an integrated biological response template developed by a team of local, state and federal emergency responders and managers from around the country. This template integrates continuous surveillance, active investigation, key decision-making, and emergency response functions. Its key medical components are modular and include neighborhood emergency help centers and acute care centers. These centers can be converted clinics, hotels or office buildings, and are designed to relieve hospitals from being overwhelmed by ill and worried well patients. The template also incorporates community outreach programs for prophylaxis, immunization, self-help at home, and telemedicine.

By using a modular design, individual units can be multiplied to care for more casualties. The cost of such preparation under this template is modest given that the main program components are planning and establishing good lines of communication. The cost of surveillance involves capture and analysis of existing data. The response asset management system (RAMS) is a computer-based emergency management tool that is being developed for day-to-day use for routine matters, and incorporates the biological response template as a contingency. The response template also relies upon the CDC s existing responsibility for establishing a national pharmaceutical stockpile. Dr. Hutchinson estimates that a best response to a biological incident may reduce death, suffering, and economic loss by 50 percent. Biological terrorism must be prevented, if at all possible.

"Biothreat Scenario," Dennis Klinman, MD, PhD

Dennis Klinman, MD, PhD, research immunologist, presented a biothreat scenario that he believes to be quite possible by the year 2025. He predicts that viral pathogens causing severe disease could be readily engineered to attack humans, animals, natural resources (oil), and crops. He suggests that not only can antibiotic resistance and immunity be modified, the virus could be designed to mutate rapidly, hindering efforts to control the pathogens spread. He theorizes that as virologists become more skilled, they may target certain gene traits that apply to certain populations or races. Dr. Klinman emphasizes that the production of a biothreat agent is not difficult. He believes there will be ready access to such technology by 2025.

An agent can be designed to be rapidly lethal but that would limit its spread. A terrorist might target troops with this, sparing the civilian population of a country. In contrast, HIV virus does not cause severe disease until several years post infection, which facilitated its successful spread through the human population.

Klinman presents the 1918 flu pandemic that killed millions as a virus which could be reintroduced into our population by a terrorist following the genetic code that is currently being created from frozen corpse samples, exhumed from frozen outreaches where they have lain preserved since dying in the pandemic. This type of infection could quickly spread, causing a "dandelion effect," as travelers disperse from an airport, for example, with this extremely communicable disease. Our present flu vaccines would not protect us. Indeed, Dr. Klinman concludes his paper by warning us that we may never be able to keep up with viral modifications, as vaccines can take years to develop.

"An Assessment of the Biological Weapons Threat to the United States," Milton Leitenberg

Milton Leitenberg, senior scholar, Center for International and Security Studies, University of Maryland, assesses the current threat in his white paper. He quotes official US government sources that list Iraq, Libya, Syria, Iran, Egypt, China, North Korea, and Taiwan as States having offensive biological warfare (BW) programs. Official Russian government sources suggest India and South Korea as under suspicion for having such programs. Israel is not a signatory of the Biological and Toxin Weapons Convention and is presumed to maintain an offensive BW program. Dr. Leitenberg writes that it is ambiguous whether Russia continues to maintain an offensive BW program.

This State capability is an important reservoir of knowledge, training, and biological agents/weapons. The US has listed five of these countries on its annual list of "State Sponsors of International Terrorism": Iraq, Iran, Libya, North Korea, and Syria. He, as well as US government experts, believe it more credible that such a state would carry out its own mission rather than trusting a terrorist group. Leitenberg reports few, if any, of the Russian scientists, among the 60,000 total workers employed in the USSR s BW program, have immigrated to terrorist states.

Historically, states have not resorted to this form of terrorism and terrorist groups have not been successful in developing them.[4]

Of the 520 incidents, since 1900, of acts to acquire or use such weapons listed by the Monterey Institute, 350 were hoaxes reported between 1997 and 1999. 44% percent of the incidents were classified as terrorist vs. 56% as criminal. Leitenberg cites CIA Director George Tenet who stated:

> we remain concerned that terrorist groups worldwide continue to explore how rapidly evolving and spreading technologies might enhance the lethality of their operations. Although terrorists we've preempted still appear to be relying on conventional weapons, we know that a number of these groups are seeking chemical, biological, radiological, or nuclear agents. We are aware of several instances in which terrorists have contemplated using these materials.
>
> Among them is Bin Ladin, who has shown a strong interest in chemical weapons. His operatives have trained to conduct attacks with toxic chemicals or biological toxins.

Leitenberg states that the past five years have been characterized by: (1) spurious statistics which include hoaxes; (2) unknowable predictions; (3) greatly exaggerated consequence estimates; (4) gross exaggeration of the feasibility of success in producing biological agents by non-state actors, except in the case of recruitment of highly experienced professionals, for which there is no evidence to date; (5) the apparent continued absence of a thorough threat assessment; and (6) what he considers, counterproductive, and extravagant rhetoric. In reaching his conclusion, Leitenberg cites statements by the United States General Accounting Office, the Monterey Institute, and the terrorism expert, Brian Jenkins.

Leitenberg concludes by stating, "if anything, it is the combination of enormous overblown official U.S. emphasis on a domestic bioterrorism threat, and the U.S. government's neglect of biological arms control that is likely to spur wider international resurgence of interest and biological weapons." Leitenberg believes that the U.S. needs to put more emphasis on a strong verification protocol for the Biological and Toxin Weapons Convention.[5]

---

[4] See Milton's paper's discussion of the Aum group in Japan.

[5] During the Dartmouth conference, the content of this paper was a source of some discussion. While some of the participants accept Dr. Leitenberg's historical analysis, other participants expressed the opinion that modern technology and rapid advances in genetic engineering presently make this threat more real year after year in the future. One scientist stated that each year he trains graduate students in techniques allowing bioengineering to create new and more virulent organisms. For a number of participants, this is simply a perverse use of biotechnology, that is revolutionizing modern medicine.

"Application of Gene Therapy Strategies to Offensive and Defensive Biowarfare," Christopher Lowrey, MD

Dr. Lowrey, Dartmouth Medical School, reviewed the principles of gene therapy. Genes are stretches of DNA that contain coding information for synthesizing proteins that perform most of the necessary functions to sustain life. Dr. Lowrey used sickle cell disease as an example in which a single base pair mutation in the DNA can lead to a severely debilitating condition. The goal of gene therapy for this disease is to replace the abnormal gene with a normal one to produce normal hemoglobin.

Dr. Lowrey lists several technical challenges to overcome. The first is the ability to efficiently transfer DNA into target cells. The second is to then "turn the gene on." There has been progress made in these areas in the past few years, and the same discoveries that are powering the science, may be useful for offensive or defensive bioweapons.

The following are some offensive uses of gene therapy. Starting with a virulent bacterium, a scientist could insert a gene to improve its drug resistance to antibiotics. One could alter the gene for a toxin (produced by a bacterium), so that a toxin would be resistant to the antidote that used to effectively counter the toxin. A third use would be an alteration of genes to elude the existing vaccines. By avoiding recognition, the agent escapes the human immune system until the body produces a new antibody. A similar idea would be to take the virulent gene sequence from an organism for which the population is well vaccinated, and to insert it into an organism that the population is not vaccinated against (immune to).

Dr. Lowrey theorizes that one might transfer a gene for a toxin found in animals, such as snake venom, into a microbe. Another possibility might be to insert multiple toxin genes to multiply toxin potential. Microbiologists could alter the infectious behavior of an organism so that the agent attaches to lung tissue rather than liver tissue. The science is at a point now that we can start to imagine developing brand-new infectious agents that are designed literally from scratch. Dr. Lowrey mentions that new technologies exist in transfer genes without microorganisms being used as vectors. DNA can be complexed to lipids (fat molecules found in cell walls) forming liposomes that can be directly absorbed by cells. Another idea that Dr. Lowrey discusses is the regulated expression of toxin genes. By using one gene to control the expression (production) of a second toxin gene, one might program an infection to lie dormant until a planned event, such as a rise in temperature or exposure to a particular chemical like an antibiotic.

Dr. Lowrey concedes that this new technology seems more applicable to offensive than defensive strategies of biowarfare. He does predict that vaccine development could be improved from the knowledge being gained in gene therapy. Genes can be identified as coding for immunologic targets on pathological organisms or toxins they produce. Once isolated, the genes could be administered to the body, which would then produce the foreign protein, eliciting an immune response that is protective to the intact organism. This approach has already been successfully applied to the development of a gene therapy based vaccine for prevention of human hepatitis B infection. While the application of this approach to defensive biowarfare would likely require many years of development to become practical, it has the potential to dramatically decrease the speed with which new vaccines are developed, increase their efficacy, and decrease their costs.[6]

"West Nile Virus Outbreak: Lessons for Public Health Preparedness," U.S. General Accounting Office (GA0) Report.

Veterinarian Tracey McNamara, DVM, Head of Pathology, Wildlife Conservation Society (Bronx City Zoo) submitted a U.S. General Accounting Office (GA0) report, "West Nile Virus Outbreak: Lessons for Public Health Preparedness," as her significant paper submission. This 1999 outbreak, in New York City, of a pathogen previously not found in the U.S. caused great fear, including concern of a terrorist attack.

This virus may have been brought to NYC by migratory birds, and is transmitted to humans by mosquitoes biting both species. Zoonotic pathogens are capable of infecting humans and animals. They represent 49% of the pathogens infecting humans and approximately 75% of newly discovered, emerging human infections. Many of the pathogens that terrorists might use are zoonotic, including anthrax, plague, brucellosis, tularemia, and the equine encephalitic viruses.

This 70-page report covers in some detail, and from the perspective of different agencies, this outbreak, which took several months to correctly identify, after dead birds were initially discovered, eventually killing 7 residents. Key findings of the report are:

1. Local disease surveillance and response system is critical;
2. Better communication is needed among health agencies;
3. Links between public and animal health agencies are becoming more important;
4. Ensuring adequate laboratory capabilities is essential; and,
5. Because a bioterrorist event could look like a natural outbreak, bioterrorism preparedness rests in large part on public health preparedness.

Wildlife, domestic animals, and zoo species may be sentinels for infections spreading to humans. While the U.S. Geological Survey tracks wildlife issues and the U.S. Department of Agriculture tracks domestic animal concerns, no federal agency is assigned to track zoo infection concerns. Many, if not most, zoos lack direct access to veterinarian pathologists and sophisticated laboratory testing. While this paper s focus is on an apparently natural outbreak primarily

[6] Another possible offensive weapon is an agent like, "mad cow disease," which Dr. Lowrey did not write about. This degenerative brain disease was discovered in British citizens in the 1980's. A current theory is that peculiar proteins named prions, that can be transferred from sheep to cows to humans, cause this disease. This obviously could be a rather frightening type of attack for which science has no answer or cure. You could transfer a gene for the prion protein to a person and once a small amount of the prion protein was made it could (at least potentially) lead to the disease. Alternatively - and probably more practically, you could infect a target population's meat supply with the agent. Britain destroyed over 4 million cattle and its meat products were embargoed for many years. While less than a hundred humans have so far died, it is unknown what the ultimate toll may be. A related disease, infecting human cannibals, can have a 30 year latency.

affecting humans, numerous birds have died suggesting that these sentinels should also guard against agricultural terrorism.

"Averting the Hostile Exploitation of Biotechnology," Matthew Meselson, PhD

In "Averting the Hostile Exploitation of Biotechnology," Matthew Meselson, PhD, Department of Molecular and Cellular Biology, Harvard University poses this conundrum:

Every major technology -- metallurgy, explosives, internal combustion, aviation, electronics, nuclear energy -- has been intensively exploited, not only for peaceful purposes but also for hostile ones. Must this also happen with biotechnology, certain to be a dominant technology of the twenty-first century?

Dr. Meselson looks ahead and sees science having the power to manipulate life including important processes of cognition, development, reproduction, and genetic inheritance. Although he is quite aware of the potential for malicious use of this power, he finds hope in the restraint displayed for the use of nuclear weapons since World War II, and chemical weapons since World War I. Chemical weapons use in Ethiopia, China, Yemen, and Vietnam, and against Iranian soldiers and Kurdish towns are among the few exceptions. The sarin gas attacks perpetrated by the Aum Shinrikyo cult in Japan in 1994 and 1995, and several relatively minor "biocrimes," confined almost entirely to the US, are an historical record that supports a lack of current interest by terrorists in using biothreats here.

Professor Meselson reviews the US research effort into biological weapons and the reasons for its renunciation by former President Nixon. In the following edited excerpts from his paper, Meselson tries to convince us of the important effect of the rule of law and disapprobation to forestall terrorist use of biological weapons. The Biological Weapons Convention (BWC) entered into force in 1975 -- the first worldwide treaty to prohibit an entire class of weapons. The Convention now has 143 state parties, the most important holdouts being in the Middle East. Unlike the Chemical Weapons Convention (CWC) of 1993, it has no organization, no budget, no inspection provisions, and no built-in sanctions -- only an undertaking by its states parties to never, in any circumstances, develop, produce, stockpile or otherwise acquire or retain:

(1) Microbial or other biological agents or toxins, whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes;
(2) Weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.

In contrast, the stringent verification provisions of the CWC, designed with the active participation of the chemical industry, require initial declaration of chemical weapons and chemical weapons production facilities and subsequent verification on-site of the correctness of the declarations. Declared chemical weapons and chemical weapons production facilities must be secured and are subject to routine inspection until they are destroyed and such destruction must be verified on-site. Facilities that produce more than designated amounts of certain chemicals deemed to be of particular importance to the objective of preventing diversion for chemical weapons purposes must be declared annually and are subject to inspection. Suspect sites, whether declared or not, are subject to short-notice challenge inspection under managed access procedures designed to protect legitimate confidential information and to avoid abuse. Experts of the Technical Secretariat of the Organization conduct all inspections for the Prohibition of Chemical Weapons (OPCW); the international operating arm of the CWC headquartered in The Hague.

In Geneva, the Ad Hoc Group of States Parties to the BWC is negotiating a protocol to strengthen the Convention, including measures for verification. There is general agreement that there should be an international operating organization similar to the Technical Secretariat of the OPCW and that there should be initial declarations of past offensive and defensive BW activities and of current biodefense programs and facilities, vaccine production facilities, maximum containment facilities, and work with listed agents. It is also generally agreed that there should be provision for challenge investigation at the request of a state party, including investigation on-site, if breach of the Convention is suspected.

In order to encourage accuracy in declarations, and to help deter prohibited activities from being conducted under the cover of otherwise legitimate facilities, some states believe that declared facilities should be subject to randomly-selected visits by the international inspectorate, using managed access procedures to protect confidential information, similar to those practiced under the CWC. Other states and certain pharmaceutical trade associations have so far opposed such on-site visits. Other important matters remain to be resolved, and are the subject of intense negotiation, including: the scope and content of declarations, the procedures for clarifying ambiguities in declarations, the substantive and procedural requirements for initiating an investigation, measures for assistance and protection against biological weapons, measures of peaceful scientific and technological exchange, and provisions affecting international trade in biological agents and equipment.

The prohibitions embodied in the BWC and the CWC are directed primarily at the actions of states, not persons. Both conventions require their state parties to take measures, in accordance with their constitutional processes, to insure compliance anywhere under their jurisdiction, including a provision in the CWC obliging its parties to enact domestic penal legislation to this effect and to extend it to cover prohibited acts by their own nationals wherever such acts are committed. Nevertheless, important as such domestic legal measures can be, neither the CWC nor the BWC seeks to incorporate its prohibitions into international criminal law, applicable to individuals whatever their nationality, and wherever the offense was committed.

Recently, interest has developed in the possibility of enhancing the effectiveness of the BWC and the CWC by making acts that are prohibited to states also crimes under international law. A treaty to create such law has been drafted by the Harvard Sussex Program. The proposed treaty would make it an offense for any person -- including government officials and leaders, commercial suppliers, weapons experts, and terrorists -- to order, direct, or knowingly render substantial assistance in the development, production, acquisition, or use of biological or chemical weapons. Any person, regardless of nationality, who commits any of the prohibited acts anywhere in the world, would face the risk of prosecution or extradition should that person be found in a state that supports the proposed convention. Such individuals would be regarded as "hostes humani generis" -- enemies of all humanity.

"MEDNET: A Medical Simulation Network," Michael Myjak, MS and Joseph Rosen, MD

Michael Myjak (The Virtual Workshop) and Joseph Rosen's (Dartmouth Hitchcock Medical Center) submission, "MEDNET: A Medical Simulation Network," is their proposal to apply advanced technology for simulation training, medical information management, and as a component of Command and Control. Their concept for MEDNET is based on existing, reconfigurable simulation system technology that could be useful for both individual and team training. Their advance simulation system is based on existing defense modeling simulation architecture using real-time infrastructure that allows interactive live simulation scenarios. MEDNET would blend the simulation technology with tele-medicine, tele-robotics, tele- instrumentation, and virtual reality technology.

Based on a Web portal interface, MEDNET has the ability to provide basic first information to a wide audience. Further advanced technology would allow a virtual reality "cave" to provide more realistic simulation immersion. A virtual reality cave is constructed with high-resolution video graphics projectors that render a 360-degree field of view totally immersing the participants. A virtual patient can be constructed using data collected from the National Library of Medicine s Visible Human project. Combined with haptic interfaces, force sensation and other sensory modalities allow medical personnel to practice on this virtual patient.

Another aspect of the MEDNET system is the ability to have a virtual clinician assistant. This would incorporate indebted intelligent tutoring systems with an integrated knowledgebase, which could provide assistance on the Internet. The virtual clinician could be a part of a medical treatment module that captures diagnostic and other medical information to give diagnostic and treatment advice. MEDNET can also capture diagnostic knowledge from events that can be later accessed to improve future training and conflict management. Mr. Myjak and Dr. Rosen s system can be useful for both military and civilian emergency management planning/training. Were an emergency to arise, it could be a useful aspect of the response. Incorporating forensics, it could become a total operations system.

"National Commission on Terrorism Report: Background and Issues for Congress," Raphael Perl

Mr. Perl, Congressional Research Service, submitted this summary of the June 5, 2000 report by the congressionally mandated, bi-partisan body to make policy and legislative recommendations for US counter-terrorism preparedness. This report is a call for more active preparation to prevent and respond to a future catastrophic terrorist attack. Mr. Perl s eight-page paper is a summary of the 50-page report presented to Congress, with Mr. Perl's research and analysis. He believes that the report will stimulate strong congressional interest when it reconvenes in January 2001. Likely areas of focus could be on a more proactive counterterrorism policy, a stronger state sanctions policy, and a more cohesive, coordinated US federal counterterrorism response.

Highlights of the report include a focus on several countries that may support or sanction terrorist activities. The Commission reviewed Greece, Pakistan, Iran, Syria, and Afghanistan for terrorist activities, calling for further United States pressure or sanctions. The report suggests that the President may want to consider designating the Department of Defense as the lead federal agency for the government's response in the event of a catastrophic attack on U.S. soil. The report calls for a detailed contingency plan to be developed for such a response. The report also calls for national terrorism response exercises, for developing plans for cyberterrorism response, for Congress and the executive branch to consolidate and coordinate budget appropriations, for full use of law-enforcement intelligence authority, and for the expulsion of suspected terrorists.

This report has raised some civil liberty concerns. The Commission suggests that carefully planned and measured restrictions in advance of a catastrophic incident may be a way to preserve, not diminish individual liberties and our democratic system. Mr. Perl's report presents many unresolved issues, including:

Who should be in charge;
How does the government and effectively utilize the variety of tools at its disposal:
How does one prioritize budget purposes;
How effective are sanctions;
What is an appropriate role for covert operations and should the ban on U.S. assassination be changed;
How can one assure the best international effort; and,
What role should the media play in a proactive counterterrorism policy?

Mr. Perl writes that there are unresolved issues that still need to be addressed. Expert advisory groups have issued reports recently on U.S. Embassy security, U.S. military installations overseas security, and the Gilmore Commission Report on weapons of mass destruction disaster consequences management. These various reports need to be reviewed, collated, integrated, and then fashioned into future U.S. terrorist response planning.

"The United States response to terrorism: Is it time to employ The 'Drug Czar' Model?" Raphael Perl and Charles Lucey, MD, JD, MPH

Raphael Perl and Charles Lucey MD, JD, MPH, collaborated on a paper asking if a "Drug Czar Model" might be an appropriate solution to remedying the charges that the current federal antiterrorism efforts waste money and lack a unified command and control system. There appear to be some striking similarities. Counternarcotics have forced local, state, and federal agencies to build operable, cooperative, inter-agency relationships, across some 50 federal agencies, for example. By giving a White House director s office authority to approve and coordinate agency budgets, strategies, priorities, planning, and overall efforts, supporters argue that more order and synergy will result in more effective response efforts. Supporters find it desirable that Congress confirms the director's appointment and holds hearings to review ongoing operations.

The paper reviews the relationship of the Drug Czar to the President s National Security Council, the Central Intelligence Agency, Office of Management and Budget, and other agencies. Perl and Lucey review the need to respond to present and evolving threats, postulating that there may be an increasing risk of Chemical, Biological, Radiological, and Nuclear (CBRN) WMD use due to a trend toward increasing terrorist violence and less state control of such groups. This office would play an important international role to integrate foreign intelligence with domestic law enforcement. Critical to threat assessment is a better understanding of the countries and cultures in which foreign terrorists are bred to operate. Perl and Lucey argue that comprehensive planning requires integrating threat assessment and domestic preparedness capabilities with the budgeting process. They warn in their conclusion that we cannot ever become complacent and must appoint such an office to take charge. We must examine where the present Drug Czar s office has been hampered in its success to improve on its proposed, sibling White House office.

Deterring CBRN Terrorism: Developing a Conceptual Framework, Michael Powers, MA

Mr. Michael Powers, Chemical and Biological Arms Control Institute, presented a conceptual framework for deterring chemical, biological, radiological, and nuclear terrorism. To arrive at this framework, the Institute examined the elements of, the opportunities for, and the instruments of deterrence. The elements of deterrence include consideration of the action to be deterred, the target, a cost benefit analysis, an understanding of motivations and values, analyzing rationality and risk aversion, communication, and U.S. credibility. Deterrence opportunities include value formation, motivation, playing/information gathering, acquisition, stockpiling, deployment, dispersal of a weapon, and the exploitation of the terrorist incident. The instruments of deterrence include awareness, denial measures, defensive measures, punitive measures, communication, and international cooperation.

Much of this paper focuses on the psychology of terrorism. We must model terrorist's motivations, values, and how they make cost benefit decisions. Deterrence requires that we recognize, identify, and track organizations/individuals who may or do gravitate towards terrorism. To understand the terrorist, we must also understand the potential targets. Decision-making is a highly complex and psychological process. The cost benefit analysis requires the analysis and weighing of many factors.

Cost can be measured in terms of punishment, financial resources, time, international prestige, internal political perceptions, and retribution. Communication with both terrorists and targets is very important. Direct communication is usually preferable to indirect channels. Engagement of the enemy can lead to better understanding, and a lessening of tensions. Credibility can play a critical role in deterrence. It may be used to establish trust or respect for a will to retaliate.

The Institute recommends that, with the quickening pace of globalization, the international community needs to implement legislation and treaties to control the spread of critical materials and equipment, like the CDC s Select (biological) Agent List. By demonstrating an effective response to the physical effects of biological agents, the potential terrorist is made aware that adequate defenses are in place. This then becomes a part of the "chain mail" of deterrence. CBACI concludes that it is possible to deter terrorists, but that there will be circumstances in which this will fail. Advanced preparation and an informed public will decrease the risk of panic should an incident occur.

"Persistence of Native and Non-indigenous Microorganisms in Winter Conditions," Michael Reynolds, PhD

Mike Reynolds, Research Scientist, US Army Cold Regions Research and Engineering Laboratory, is investigating the "recovery ability," or decontamination, of soil following release of chemical and biological agents. His group s background is in soil microbiology, soil chemistry, and modeling. In their research, they try to treat the soil as a system that contains not only microbiology, but also chemical, physical, climatic, and vegetation related influences. Reynold s group is trying to understand the persistence and fate of biological agents that may be released, especially in a cold or winter setting. They have found that decontamination procedures for most hard surfaces are much less successful in treating soil. Dr. Reynolds is using endospores, which persist in cold soil, as a model to try to improve biological cleanup, using knowledge gained from cleaning up organic compound spills. The following are known methods of decontamination:

Thermal oxidation, "dig it up and burn it" to,
Chemical oxidation "dig it up and wash it with a strong oxidant", to
Biological oxidation, "dig it up and put it in a bioreactor", to
Natural attenuation "natural processes will remediate many sites", and finally to
Enhanced natural remediation "lets understand the system so we can manipulate it to give natural processes a significant boost".

Dr. Reynolds group is in the early stages of investigating the potential of altering the soil s microbial community to maximize the competitive advantage of native microorganisms over introduced microorganisms. They have found ways to alter the soil s microbial community, with low-cost, readily implemented actions. This may be important knowledge in planning responses for both human and agricultural terrorist targets.[7]

---

[7] There has been some application of this basic research. The September 26-28, 2000 USAMRIID (US Army Medical Research Institute of Infectious Diseases)/ FDA Satellite Broadcast on Biological Warfare and Terrorism, mentioned a recent, extensive efforts to decontaminate an island used for anthrax testing, years ago. Panelists noted that it was unknown whether such an effort was required scientifically, but certainly reassured the public. A recent NOVA report, broadcast October, 2000, on prions (mad cow disease or spongieform encephalitis) notes that infectious material (brain), buried in a garden for three years, remained infectious.

"Bio-Medical Aspects of Bio-Terrorism and a Call to Action," Paul Roth, MD, Brian Hjelle, MD, and John Gaffney, BBA

Paul B. Roth, M.D., Dean and Professor of Emergency Medicine, Brian Hjelle, M.D., Associate Professor of Pathology, Infectious Diseases and Inflammation Program, and John K. Gaffney, BBA, CEM, TEMT-P Director, Emergency Planning and Operations University of New Mexico, School of Medicine, believe that it is becoming more likely that we will face a biological terrorist act for several reasons. One is the psychological impact of this type of threat. The unseen, and in all other respects, undetected attack makes for a very effective terrorism weapon in and of itself.

Even the most conservative are alarmed by the incredible advances in biotechnology. It is now possible to alter the most virulent bacterium or virus and make it both more pathogenic and less likely to be killed by conventional therapy. The molecular biology revolution has now been underway for more than three decades, and the sheer number of persons with dangerous technical expertise has increased exponentially since the 1960s.

The authors write that the challenges facing our ability to effectively defend against bio-terrorism are much greater today. There are more high-density population centers within the United States that may be exposed to these agents. Due to increased mobility, infected individuals will spread these genetically altered organisms -- with their high rate of mortality and/or morbidity -- with great rapidity.

Roth, Hjelle, and Gaffney believe the current efforts to develop these defenses are uncoordinated and lacking vision. There are hundreds of millions of dollars that have been appropriated to address a number of aspects of this defense but there does not appear to be a well-defined strategic plan directing these efforts. They write that the scientific community could benefit from a national effort to develop methods of early detection and customized, rapid treatment strategies (vaccines, anti-viral, and/or other drug therapies). Roth, Hjelle, and Gaffney advocate shifting money from federal response efforts to support community training and equipping of first responders and health care providers, where the responsibility for an initial response to a Weapon of Mass destruction (WMD) event will lie.[8]

As an example of such a cooperative effort, they describe how the University of New Mexico School of Medicine has formed a coalition with Los Alamos National Laboratories (LANL), Sandia National Laboratories, the New Mexico State Department of Health, and Lovelace Respiratory Research Institute. Among the first projects is the development of a model for population surveillance for early detection of a terrorist attack. Surveillance would be accomplished through the utilization of real-time computerized reporting by health professionals in an

[8] As other of the conference experts have suggested, the New Mexico team advocates collaborative programs between federal and state governments, the private sector and academic institutions on the scale of World War II's Manhattan Project. The problems described above that are associated with bio-terrorism pose a level of complexity many orders beyond that of simply developing an atomic weapon.

emergency department. All patients with presenting complaints consistent with a flu-like illness would be reported to the surveillance network. This will serve as an efficient model for rapidly detecting new clusters of infections in a population, and to develop the informational tools and datasets for developing the ability to distinguish natural from humanmade outbreaks. The model could yield immediate practical public health benefits such as the identification of early outbreaks of naturally occurring illnesses caused by influenza, enteroviruses, or the respiratory syncytial virus.

There are pilot projects to develop ultra sensitive biosensors for directly detecting pathogenic viruses in the environment. One project uses near-infrared spectroscopy to detect changes in cells that may mimic the changes that occur very early in the infection of an animal. An NIH grant is being sought to further expand the effort toward early detection of exposure to biothreat agents utilizing genomic microarray technology. The School of Medicine s Infectious Diseases and Inflammation Program (IDIP) is using the Consortium s expertise to train a new generation of basic scientists. Future requirements for scientific leadership will require highly interdisciplinary, broad-based training in infectious diseases and immunology

Roth, Hjelle, and Gaffney cite one special current need -- more Bio-Safety Level 4 (BSL-4) labs. These laboratories are designed to allow scientists to safely study the lethal organisms that bioweaponeers are most likely to release. Currently, these high-containment labs are located in only a few areas in the country with limited access by the general scientific community. At this time, there are four of these laboratories located in this country (NIH, Bethesda, Maryland; CDC, Atlanta, Georgia; US Army Medical Research Institute of Infectious Disease, Fort Detrick, Maryland; and Southwest Foundation for Biomedical Research, San Antonio, Texas). Prior to two years ago there were only two Level 4 labs, and they were for the most part restricted to government use. Although there are four more labs being planned (three in Texas and one on Plum Island, New York) access and therefore scientific discovery will remain limited. Even if all of those planned facilities are built, the US will still be markedly lacking in the high-throughput vaccine and therapeutic testing capability that is crucial if we are to meet the threat of a bioweapon attack.

The New Mexico team lists five priorities for future efforts. First, further research is needed in the fields of microsystems for the development and wide distribution of devices for the early detection of selected organisms in the environment. Second, research is necessary in bio-medical sciences to rapidly recognize individuals who are infected with bio-threat organisms and to develop customized therapies. Third, to slow and eventually halt the spread of these bio-terrorism agents there must be rapid containment strategies and facilities. Fourth, mass training of first responders and health care providers who may be called upon to deal with these types of situations in local communities must be developed and implemented. Last, there should be a special blue-ribbon panel created composed of federal, state and local government representatives, members of the scientific community (private sector, national laboratories, and universities), and private industry to plan a unified strategy to defend the American people against this imminent threat. Thereafter, a similarly unified structure must be developed and empowered to implement this strategy.

"Chemical and biological (CB) weapon terrorism: assessing the challenges from sub-state proliferation," Jean Paul Zanders, PhD

Dr. Jean Zanders, SIPRI (Stockholm International Peace Research Institute) writes from the perspective of a sub-state entity, which may be a company, an individual, or an organization, in contrast to an international operative. Terrorism has been practiced across all types of civilizations and throughout history. Poisonous substances have been used for assassination, including biologic agents like ricin (including recent use by state agents). Dr. Zanders points out these opportunity costs to acquiring biological agents: funding, resources, public opinion, environmental, international law and disarmament treaties. Analyzing the terrorist organization s social environment can assist in assessing the threat from biological weapons. One needs to look at the tension between the threat perception and the norms that govern its behavior. Dr. Zanders states that the greater the existential threat to the terrorist, the greater the chance of its resorting to extreme measures. Dr. Zanders discusses the difficulty of identifying norms, as they are relative to state vs. nonstate, religious vs. political, continuing coexistence vs. extinction, etc. Even international law allows withdrawal clauses in treaties and extreme measures to protect the survival of a state. He suggests that a biological terrorist strike is definitely feasible, but with the caveat that there are major impediments to the acquisition of the weapons. For example, there are technical barriers to producing the amounts required to cause mass casualties.

Much of the analysis of the threat of terrorism with CB weapons has so far been directed toward circumscribing the threat, profiling organizations likely to resort to such weapons and investigating the requirements for consequence management. However, once it has been determined that a particular group has developed an interest in chemical or biological weapons, its eventual acquisition and release of these weapons is virtually taken for granted. With nuclear weapons as the yardstick, CB weapons are seen as easy and cheap to obtain. Dr. Zanders argues this black box approach has diverted attention away from what is actually involved in the acquisition of chemical or biological weapons by a terrorist group. A terrorist strike with chemical or biological weapons is definitely feasible. Aum Shinrikyo demonstrated as much in 1995. Nevertheless, the likelihood of such an event recurring must be judged on the basis of realistic and testable parameters.

The paper applies the "assimilation model" for the demand-side study of CB weapon proliferation in states, to sub-state actors. The model draws attention to the many thresholds that the terrorist organization must overcome, and the opportunity costs they are willing to pay to overcome these thresholds in order to complete the armament dynamic.

Chemical and biological weapons only make sense in relationship to specified goals. To Aum Shinrikyo they represented two possible avenues to the ultimate goal of destabilizing Japan and taking over the government. They were to be used in conjunction with other exotic or devastating weapons, as well as with ordinary conventional firearms. (Arguments such as ease of production or relative cheapness merely have a bearing on how certain thresholds are overcome in the pursuit of these goals. In the case of Aum Shinrikyo these factors were arguably of limited importance in view of the massive investments in the other weapon programs. They may have played a role in the sequence in which the various armament programs were launched.) Had the sect focused exclusively on CB weapons, it would have probably solved the problems of viability of the chosen pathogens, large-scale production of chemical and biological warfare agents, and effective dissemination. However, such an exclusive focus would not have served the totality of the final goals. Consequently, the sect had to engage in the politics of priority allocation of resources and the CB weapon programs had to compete with the other weapon projects. Factors that increase the aggregate opportunity costs for weapon programs, such as rivalry between leading sect members, influence peddling, and so on, were also observable in Aum Shinrikyo. The outcome was many unresolved issues in the CB weapon programs as well as in the other weapon projects.

The material (financial) base upon which Aum Shinrikyo could draw was huge and few other terrorist organizations will be able to match it, however, the cult s failures and difficulties are significant for the threat assessment of terrorism with CB weapons. Variations in the composition of the material base have an immediate impact on the ability of an organization to successfully sustain a CB weapon armament dynamic. For instance, only a vertically organized, highly integrated and ideologically uniform group appears to have the capacity to set up and operate a large-volume production line for chemical or biological weapons in absolute secrecy. Religious sects, more than any other group, come to mind. This definitely reduces the number of candidates that could sustain such an armament program. The high technical hurdles ultimately limited the range and affected the quality of the warfare agents Aum Shinrikyo was able to develop. Military-grade warfare agents therefore are unlikely to constitute the main threat.

Nevertheless, the constraints in the material base can lead to a low-volume, high-quality manufacture of chemical or biological warfare agents. Loosely structured or cell-based terrorist groups or even lone individuals can produce small quantities of such agents. Dr. Zanders concludes that while this broadens the possibility of these agents being used in terrorist attacks, the small quantities are unlikely to result in mass casualties.[9]

"Mobile Code: Emerging Cyberthreats and Protection Techniques," Jian Zhao, PhD

Dr. Jian Zhao , Director, Digital Security Technology, Fraunhofer Center for Research in Computer Graphics, Inc., writes on mobile code, which is computer programming code that is downloaded to a device attached (or connected by wireless communication) to a network. This happens in the course of an interaction between the device's user and the network (or another

---

[9] This paper shares some similar, conservative, reasoning with Milton Lietenberg's and Mathew Meselson's cautious approaches. Dr. Zanders does not comment on the ability of Bin Laden, who may be worth 250 million dollars, to carry out his threatened religious war. Nor does he comment about whether any of the increasing number of post-doctoral researchers, that Dennis Klinman says are leading the biomedical laboratory revolution, constitute intellectual capital upon which terrorism may rely instead of financial capital. The assimilation model would clearly recognize this as a factor. While Dr. Zanders rejects the idea that there wil be widespread use of CB agents by terrorists, he does allow that a dedicated effort could produce them, perhaps to be employed on livestock, crops, or a target less morally apprehensible.

device attached to the network) and is then executed as part of the interaction. Mobile code is ubiquitous on the Internet, though many people do not realize that their computer is using it.[10]

The following is an example of how mobile code is useful for robots. A robot operator can send mobile code (instructions) to a robot in the field to dynamically change the robot s behavior, so that the robot can better handle the exact task at hand. The robot may even change roles, perhaps switching from policeman to nurse at a contaminated site. Hence, the robots also must be protected from malicious mobile code.

Java or ActiveX are two popular programming languages for these applications. Jini is a promising technology based on Java, providing simple mechanisms that enable various devices to plug together to form a community. Developed by Sun Microsystems, it may one day allow all home appliances to communicate over a network with the inhabitants to better run the house. Each device provides services that other devices in the community may use. Mobile code is also used to implement features in devices such as cellular telephones. When a user accesses one of these features on a cellular telephone, mobile code for the feature is downloaded to the cellular telephone and then used in the interactions that involve the feature. When mobile code becomes an autonomous program and travels from host to host on a network, it evolves into mobile agents. Compared to mobile code, mobile agents typically move from host to host to accomplish specified missions autonomously and collaboratively.

Robots and other remotely controlled devices could play a critical role both during the attack and in the response phase after the direct bio-attacks. In both cases, they face a hazardous and hostile environment. Because of their natural immunity to biologic agents, terrorists may attack these systems via mobile code sabotage. Such protection involves intrusion-detection systems, strong encryption for all communication, and trained human analysts to monitor computer and robot behavior. Such protection involves a combination of traditional techniques (e.g., digital signatures) and techniques that are still under development (e.g., code "sandboxing," where a program is confined to a sanitized space as its code is checked for viruses, before allowing it to access system components).

"Possible terrorist use of modern biotechnology techniques," Raymond Zilinskas, PhD

Dr. Raymond Zilinskas's [Monterey Institute of International Studies (MIIS)] paper results from a collaboration between the Center for Nonproliferation Studies at MIIS and the Center for Counterproliferation Research at the National Defense University (NDU) to assess the likely impacts of recent and anticipated advances in biotechnology on the ability of terrorists to acquire

---

[10] For example, while one has to download a program before using Net2phone to place calls on the Internet, Dialpad (another phone service) sends a Java applet (small self contained program) to operate on your desktop, only as you are logged onto the site.

and deploy biological agents for criminal purposes. Dr. Zilinskas abstracted the assessment s findings in three areas: 1) identifying which advanced biotechnologies are available, and are likely to become available in the next five years, to scientists and technicians working as or for terrorists; 2) analyzing how these advanced biotechnologies may be used to enhance attributes of microorganisms for purposes of warfare and terrorism; and, 3) draw conclusions and make recommendations as to what may be done to decrease the likelihood of the advanced biotechnologies being used for illicit purposes.

There are five attributes considered important for agents used for purposes of biological warfare. They are high virulence coupled with host specificity, substantial degree of controllability, considerable resistance to adverse environmental forces, lack of timely countermeasures to the population to be attacked, and ability to camouflage the agent with relative ease. The assessment discusses the capacity of scientists to modify these attributes. It characterizes virulence as the ability of a pathogen to quickly cause severe damage (the smallpox virus and Bacillus anthracis are examples of virulent pathogens). Virulence can be expressed locally, systemically, or via evasion of host defenses. An example of local virulence is the destruction of tissue near the initial infectious focus, by the so-called "flesh-eating" bacteria, Group A Streptococcus. The secretion of toxins into the circulatory system usually produces systemic effects such as shock. Evasion of host defenses may result from special encapsulation of the pathogen, enabling it to be unrecognized by phagocytes. Also, some bacteria and viruses can hide within the host s cells, thereby evading the host's immune response.

The assessment posits that it would be fairly easy for a properly trained junior scientist to identify genes coding for many of the well-characterized virulence factors and to transfer them into bacteria and viruses being developed for weapons use. However, a little-known factor, pleiotropism, can be a substantial important barrier to the usefulness of genetic engineering in the weaponization process. Pleiotropic effects are unwanted and unplanned characteristics, such as reduced hardiness or virulence that may accompany the deliberate alteration of an organism s genome for purposes of weaponization. If a pleiotropic effect were to appear it could make the genetically altered agent unsuitable for weapons purposes. Since it is possible that any attempt to weaponize a microorganism through the use of genetic engineering would result in the appearance of one or more pleiotropic effects, the end product requires extensive testing to evaluate its potential for biological warfare. If testing reveals a detrimental pleiotropic effect, another cycle of research, development, and testing is required to get rid of that effect while retaining the attributes valuable for warfare.

In the assessment, some genetic alterations that scientists could possibly perform for the purpose of weaponizing microorganisms are described. For example, it is possible to limit the spread of a contagious pathogen by using suicide constructs. Scientists have designed genetic constructs that program the death of the cell into which they are placed under specified conditions. These constructs typically include a gene that codes for the production of a toxin and a promoter sequence that activates the toxin gene in response to a precise signal, such as a change in temperature or the presence of a chemical stimulus. A similar genetic mechanism could be used to program deliberate senescence; that is, cell death, after a bacterium has undergone a certain number of cell divisions or a virus has passed through a certain number of host cells. The assessment also discusses the possibility of deliberately causing a pathogen to enter a viable but non-culturable condition; a dormant state during which it cannot be detected. Once the attacker provides the proper cues, the dormant organism reverts to its active, pathogenic state.

One of the conclusions of the MIIS/NDU assessment is that by the year 2005, scientists will be able to genetically engineer bacteria for purposes of warfare by, for example, increasing their resistance to antibiotics, adding virulence factors, altering their antigenic presentation and, possibly, controlling the viable but unculturable condition. There are two likely scenarios for the use of advanced biotechnologies, especially genetic engineering. The first scenario involves state-supported terrorists. State programs have the funding and qualified staffing to undertake the type of difficult, risky research employing genetic engineering. Further, they are more likely to perform adequate field-testing of weaponized agents than non-state actors. A state might arm its dependent terrorist group with sophisticated biological weapon for two reasons. First, the state-supported terrorists could initiate a destructive biological attack prior to the state sponsor beginning a conventional attack against an adversary nation. Second, the state-sponsored terrorist group may use mass casualty biological weapons against an enemy state that possesses an overwhelming conventional or nuclear capability.

The second scenario involves a disgruntled or deranged scientist or technician. Often, these types of persons work in a well-equipped clinical or industrial laboratory. While performing their normal work, it is possible for them to secretly develop sophisticated pathogens for use against hated persons or entities. Alternatively, they may employ pathogens to blackmail or destroy agencies and businesses. This, the microbiological equivalent of the Unabomber, would be the most difficult type of terrorist to deter, detect, and apprehend.

Other than state-supported terrorists and disgruntled or deranged scientists/technicians, it is unlikely that other types of terrorists will find the advanced biotechnologies useful for developing biological weapons. In particular, the ever-present possibility of pleiotropic effects hampering the weaponization process of any pathogen will deter the widespread use of genetic engineering by scientists and technicians working for non-state actors. However, because modern biotechnologies are advancing so rapidly, assessments such as the present MIIS/NDU need to be performed every two years. In particular, the timeframe of 2005-2009 is most worrisome in terms of advanced biotechnologies being utilized for purposes of terrorism and criminality.

Conclusion

These white papers illustrate the range and diversity of opinion that fuel the debate regarding possible biological weapons use by terrorists within the next few years. Peering out to the year 2025, it is clear that rapidly advancing science and its dissemination pose a credible threat potential. Some participants see the ability to employ such weapons spreading from nations, to groups, and ultimately to individuals, as we have seen with mail bombings by the Unabomber and the Oklahoma City Tragedy. Defensive capabilities must be continually updated and made more sophisticated to address biological vectors, information cyberterrorism, and other technology in its infancy, such as nanotechnology. Resources can be channeled into cooperative efforts to study and apply biological research, information technology, computer simulation and virtual reality systems, and robotic response technology. This effort must also extend to agricultural and industrial applications. Most of the research and investment has dual uses for positive outcomes, including improving our public health structure. We know from military technology applications that it takes years for advanced projects to be developed into working prototypes. These papers stimulate such advance planning for the years up to 2025.

Advances in Biotechnology:
Promise and Peril

George Poste
Health Technology Networks
Washington, D.C. 28 Nov. 2000
The Technological Foundations of National Security Threats

Historical:

- "big bang — big metal"
  - physics and engineering
  - high profile signatures for IC

Emerging

- "cyberwarfare"
  - ubiquitous connectivity
  - few forensic signatures and no warning
- "bio"
  - biotechnology changes the rules
  - biology loses its innocence
  - increasingly complex dual-use dilemma

The Promise of Biotechnology: Molecular Medicine and Increasingly Individualized Care

The Perils of Biotechnology :
Dramatic Amplification of Dual-Use Applications for Bioterrorism and Biowarfare

‘ FIGURE: See Attached File

Figure: See Attached File

(predictive biology)

New Dual-Use Technologies with Potential Applications in Biowarfare and Bioterrorism

- ID of new molecular targets for bioagents
    - humans, animals, plants
- genetic control of microbial virulence and engineered pathogens
    - expanded tissue or host ranges
    - new modes of spread
    - circumvention of current Dx, Rx, Vaccines
    - hypermutable agents
    - evoked over-production of cytokines (shock)
    - hybrid agents
    - recombination agents
    - latent, integrated agents and activation systems

New Dual-Use Technologies with Potential Applications in Biowarfare and Bioterrorism

- expanding definition of bioagents
    - more than just bugs
- directed dysregulation of specific genes and gene circuits
    - reversible immobilization or catastrophic effects (acute/chronic)
    - activation of inflammatory cascades
    - triggered neural pathways
        * violence, lethargy, depression, addiction
- comprehension of biological control mechanisms creates new class of C (chemical) agents

New Technologies and the Escalating Complexity of BWC Surveillance and Inspection

- dramatic expansion of dual-use facilities
- new analytical methods and technical skills
    - diversity, sensitivity
    - remote, on-site
    - cyber-forensics
- nature and ID of other biological agents under the General Purpose Criterion
    - gene therapy vectors, gene transcription regulation, evoked dysregulation of homeostatsis
- confidentiality and privacy protections for legitimate proprietary commercial assets

The Multidimensional Face of the "Bio" Problem

- from devastation (millions of casualties) to repetitive disruption (PSYOP; economic impact)
- multiple agents, multiple targets, multiple environments

widely differing scenarios

FIGURE DELETED: SEE ATTACHED FILE

wide spectrum of defensive postures

paralysis and inaction?
or
purposeful-threat reduction?

Difficult problem = YES Too hard a problem = NO

Using New Knowledge About Bioagent Fingerprints to Build Better Detection and Diagnostic Capabilities

Genomic and Proteomic Profiling of Bioagents and Conventional Pathogens

- technology foundation for novel, rapid diagnostic tests (Dx)
- simultaneous profiling of natural or engineered Rx or immune- resistance or other atypical markers
- archiving of global samples from natural epidemics/epizootics
- profiling of FSU bioagents
- inventory molecular signatures from organisms used in legitimate commercial activities
- parallel value as public health resource

The Diagnostics Dilemma in Medicine

- common diseases are by definition the most frequent
- "If you hear hoof-beats it is more likely to be a horse than a zebra"
- many bioagents will first produce flu-like symptoms
- how can the presence of a bioagent (zebra) be detected in a large background noise of routine infections (horses)?
- non-intrusive Zebra test that fits into routine medical procedures

The Zebra Chip

- build on rapid private sector development of "gene-chips" for medical diagnostics

Zebra Chips Deliver More Than Just Rapid Bioagent ID

- fundamental element of infection control and improved triage
  - ID of presymptomatic infected patients
  - expanded monitoring of exposed at risk population
  - superior triage in allocation of scarce Rx
- critical information for improved disease management
  - faster ID of bioagent faster use of The Right Intervention
  - disseminate simultaneous information on optimum Rx
  - information on any other unusual features of the bioagent
- focused, less disruptive, quarantine controls
- forensic attribution and enhanced deterrence
  - unique bioagent signatures related to geography and/or production process

Making Diagnostic Data Actionable in Real Time

IC — DOD — Civilian Interfaces

Medical Response to BT/BW Attack

Radical Re-Engineering of Pharmaceutical and Vaccine Manufacturing Processes

- rapid mobilization against unexpected threats (natural or engineered)
- surge, on-demand manufacturing
- genomic/proteomic profiling and "predictive immunology"
  - epitope ID, TH1 vs TH2 epitopes
- synthetic vaccines : converting biological processes to chemical syntheses
  - drugs = chemical
  - vaccines = biological
  - synthesized epitopes = fast cycle times
- regulatory complexities
- biotechnology and systems biology are classical dual-use technologies with beneficent and malignant applications
- the relevance of life sciences R&D for national security will increase dramatically
- the ubiquity of biotechnology and open-source data will increase the probability of its use of terrorists
- increasingly powerful methods to manipulate microorganisms and and human body function will expand the repertoire of bioweapons available to sophisticated adversaries
- the US and its allies are highly vulnerable to attack by traditional and novel bioagents
  - major technical, medical, political and organizational shortcomings
- modern biotechnology and computing provide powerful platforms to deploy a comprehensive surveillance network of diagnostics for faster detection of a bioattack or suspicious atypical incidents
- effective drugs and vaccines are lacking for most classes of bioagents
- new R&D and manufacturing methods are needed urgently to address these vulnerabilities
- new technology initiatives in diagnostics, therapeutics and vaccines for bioagents will generate enormous parallel benefits in strengthening global public health capabilities
- such initiatives are vital in preparing for the resurgence/emergence of naturally

occurring epidemics on a global scale and in limiting their medical, economic and political consequences

FIGURES DELETED: SEE ATTACHED FILE

• 10^4-10^6 simultaneous tests
• ID the bioagent
• profile the stain
• profile Rx sensitivity/resistance

• miniaturized
• automated analysis
• rapid analysis (<1 hr)
• automated readout

• direct interface to medcal data network for rapid alert and early action

Data Collection

Computational Network and Alerting System

- Z-chip networks
- other indicators
  - syndromic
  - epidemiologic
  - environmental
  - IC inputs

- data standards
- robust analytical and mining tools
- networked
- incident management tools
- C^2 capabilities

Medical Management

The Drug and Vaccine Supply Chain

drugs/vaccines

- no surge capacity for excess production
- inadequacy of Rx/Vaccine stockpiles
- lack of incentives for private sector engagement
- R&D
- supply
- DoD underestimation of JVAP resources needs/cost
- unclear FDA policies

no drugs/vaccines developed

- vulnerability to large number of biothreats
- major gaps in antiviral drugs
- need for radical investment in R&D for drugs/vaccines
  - DARPA
  - engage private sector

Future Strategic Issues/Future Warfare [Circa 2025]
D.M.Bushnell

- Capabilities of the "Enemy After Next"
  - -Ongoing Worldwide Technological Revolutions
  - -Economic Trends
- Potential Nature of Farther Term Warfare

"Going In" Assumptions

- Politics can/does change "overnight" [e.g. Russia, Iran, Iraq, Pakistan etc.],Potential CAPABILITIES is the future warfare issue, not Who but WHAT
- Order of 10+ years required to develop/field new systems, in inventory for 30+ years, should be designed for middle of inventory period, hence 2025 time period

Technological Ages of Humankind

- Hunter/Killer groups [Million BC~10K BC]
- Agriculture [10K BC~1800 AD]
- Industrial [1800~1950]
- IT [1950~2020]
- Bio/NANO [2020-?]
- Virtual

Currently

- Order of 70% of Worlds Research Conducted outside of U.S. [to first order, a % of GDP, U.S. produces order of 18% of worlds GDP]
- Order of 70% of U.S. Research now "Commercial" [as opposed to Government spon sored]

Worldwide IT Revolution

- Comms/Computing/Sensors/Electronics
- U.S. Commercial IT R&D ~ $100B/yr.
- Factor of 1 Million further improvement [Silicon, Molecular, Quantum, Bio, Optical]
- Beyond Human AI?
- Automatics/Robotics "in the large"
- Immersive multi-sensory VR/"Holodecks"
- Ubiquitous multi physics/hyperspectral sensors [land/sea/air/space]
- Micro/Nano sats/GNC/sensors, etc.

[Worldwide] Impacts of Ongoing IT Revolution Upon Society

- Tele-commuting
- Tele-shopping
- Tele-entertainment
- Tele-travel
- Tele-Education
- Tele-medicine
- Tele-commerce
- Tele-politics
- Tele-socialization

Inexpensive Motivational Asynchronous Web-Based Distance Education Enables:

- Demise of the U.S. "underclasses"
- Wealth Creation from enabled "Invention"
- Stabilization of World Population
- [Even More] Rapid Technology Diffusion
- Equalization of "Haves" and "Havenots"
- Altered Political/military outlooks Worldwide - I.E. Changes "Everything"

"In this [Worldwide] economy our ability to create wealth is not bounded by physical limits/resources but by our ability to come up with new ideas"

[However, even "universal wealth" will not obviate the other causes of warfare which include Politics, "Face", Religion, Megalomania and Territorial Disputes]

Current Competitive Landscape

- U.S. produces only 18% of Worlds GDP
- ~70% of Research conducted offshore
- $300B/yr trade deficit
- 32 other nations devote a larger % of their GDP to Research
- 5th in No of R&D personnel/labor unit
- 3% savings rate vs. 30% in Asia
- Proliferation of IT, bio, nano, Space Technology etc.

Bio Revolution Applications

- "Pharm Animals" [drugs, spare parts]
- Fast Growing plants on/near sea surface & sea water irrigated plants for biomass energy/closed CO_2 cycle
- Polymer growing plants
- Spider genes in goats allow spider silk spinning from goat milk for "Biosteel", 3.5X strength of aramid fibers for Armour
- Binary Bio-weaponry

Summary - Major Influences of IT/Bio/Nano upon Future Warfare

- Ubiquitous miniaturized/networked multi physics, hyperspectral sensors
- Robotics/Automatics "in the large"
- Long range precision strike/targeting
- Info/net Warfare
- Mini/micro/nano Sats, Cruise, UAV s
- Binary Bio Weaponry
- Miniature/ubiquitous "smart mines"

Carbon Nanotubes

- C1,000,000,Buckminister Fullerine Carbon
- 100X strength, 1/6 weight of steel
- 8X better Armour
- Low energy Molecular/Petaflop Computing
- Ultra Capacitor/High Temperature SC
- Non-Cryo H2 storage

Aluminum/Vortex Combustor

- Micro powdered Aluminum fed into a vortex combustor "burns" SEAWATER
- Provides AIP with high energy density/efficiency for:
  - -inexpensive SS with "near SSN" perf.
  - -Transoceanic UUV s
- Would allow "Enemy After Next" to AFFORDABLY Threaten CONUS via Multitudinous in-shore short-time-of-flight "popups"

"Volumetric" Weaponry -[Alternatives to HE]

- EMP
- Info/Net/Psy warfare
- Miniature brilliant sensor/mine combo s
- Fuel/air & dust/air
- RF
- Chem/bio Antifunctionals/antifauna
- Isomers, Strained Bond Energy Release, etc.
- Carbon fibers/Acoustics etc.

Then Year Targeting/Connectivity etc.

- <u>MILITARY</u> overheads/systems
- Ubiquitous <u>COMMERCIAL</u> overheads/systems
- <u>SCIENTIFIC</u> overheads/systems

  IN the context of:
  - Inexp. Reconstitution via micro/nano sats
  - Optical comms /GPS etc.
  - Ubiquitous inexp. UAV/HALE adjuncts

Blast Wave Accelerator

- Global Precision Strike "On the Cheap"
- No barrel,~100 ft. notched rails ,sequentially detonated Distributed HE
- Mach 27 or less as desired, up to 3000 lb
- Base anywhere,~$200/lb of projectile
- Excellent stealth [no plume] ,affordability, ferocity, reaction time, survivability, recallability, effectiveness
- Being worked at Aberdeen and NASA MSFC for lofting of Fuel and Nanosats

[Agreed Upon] Assumptions, Combat in 2025

- Proliferation of TBM s, IT, Precision strike/targeting, ubiquitous micro sensors, camo/spoofing, robotics, bio/chem munitions
- Logistic assets highly vulnerable in or out of theater
- In and near theater ports/airfields possibly unusable
- Beam weapons increasingly prevalent

Potential En-route Logistic Vulnerabilities

- <u>Logistic</u> surface ships and aircraft are <u>non-LO</u> and <u>undefended</u>, could be targeted and attrited inside the continental shelf by:

  -"Eggs" [subsurface floating encapsulated missiles implanted by freighters/SS/air]
  -SS [torps/missiles/subsam]
  -Transoceanic UUV s,UAV s
  -Blast wave accelerator
  -Cruise,TBM s
  -MINES

Fundamental Problem With Future U.S. Power Projection

- "EAN" can have "country sized magazines" filled with hordes of inexpensive Precision strike "Munitions" - Area Denial
- U.S. Forces run out of "bullets" and die

[Beam weapons not panacea, inexpensive workarounds available]

- Deep Water Subs with large loadout/"swimin" weaponry only survivable "Close-in" platform

Example Then Year" Direct Conus Attack Capabilities

[~80% of CONUS population/infrastructure within ~ 50 Miles of a "coastline"]

- Inexp. Transoceanic UUV s/UAV s/Cruise
- Inexp. Blast Wave Accelerators
- Inexp. Info/Net/Psywar
- Inexp. Inshore AIP SS [mines/torps/SLCM]
- Inexp. Binary Bio into Food Supply
- Inexp. Semi-submerged Missile "eggs"

Example Then Year" Direct Conus Attack Capabilities (continued)

- Trojan Horse" "civilian" systems

[Above in addition to ICBM/TBM]

Future Warfare "On The Cheap"

- Info/net warfare
- Binary bio [anti-functional/fauna]
- Non-lethals
- Miniature brilliant sensor-mines
- Micro/Nano Sats
- LO/Long leg/precision UUV s/UAV s/Cruise
- Inexp./Superb/survivability ISR/comms
- Blast wave accelerator

"Then Year " "Peer Competitors"

Peer Competitor no longer defined by "megatonnage" of obsolescent Industrial age steel and aluminum Artifacts,The Drastically reduced entry investment enabled by "Warfare on the Cheap" ensures almost any nation or sizable organization can be a very worrisome Military "peer"

Fundamental Military Issues/Metrics

- Affordability ["Warfare on the Cheap"]
- Survivability ["Can see everything , Anything you can see you can kill"]
- Effectiveness [Lethality of Precision and Volumetric weaponry]

I.E. Simultaneous ongoing Revolutions in all three of the major Warfare Metrics

Trends Summary

- Tele-everything
- U.S. just "one of the crowd" economically
- "Warfare on the cheap", many potential "peers"
- Warfare Increasingly Robotic
- Survivable/Affordable power projection via deep water subs and Blast Wave Accelerators
- CONUS and Logistics Defense increasingly worrisome

Terrorist Attack on Hanover, NH
Biological Terrorism in the Year 2000

The Terrorists

- Transnational, State Sponsored
- Long History of conflict with US
- Objectives
    - Retaliation for past US attacks
    - Punish US for "inhumane acts"
    - Demonstrate capabilities
    - Gain world-wide attention

The Target

- Dartmouth College/Hanover
    - "Soft" target
    - Difficult to isolate after attack
    - Concentrated population
    - Links to US national defense
- Auditorium on 20 September
    - 400 Students
    - Confined area

The Weapon

- Pneumonic Plague
    - Highly lethal (untreated < 100%)
    - Contagious
    - Difficult to diagnose
    - Unstable; little residual contamination
- Aerosol Dispenser
    - Small, backpack dispenser
    - Carried into auditorium
- First symptoms occur in 1-3 days
    - Fever, cough, sputum, chills
    - Similar to cold or flu
- 48 hours after initial symptoms
    - Severe bronchitis, blood sputum, chest pain
    - Abdominal pain, nausea, diarrhea
    - No buboes
- If not treated early (within 18-24 hours of onset of symptoms) death is likely

The Effects

- Nothing unusual noted 20-22 September
- By September 23 (D + 3):
    - 21 students admitted to hospital with severe respiratory infection or pneumonia (15 deaths)
- By September 25 (D + 5):
    - Hundreds of students and locals suffering from severe respiratory infections (103 deaths)
    - 50% of Hanover emergency services and hospital staff infected
    - Outbreaks in Boston, New London, UNH.
- By 27 September
    - Nearly 5000 with severe symptoms in Hanover
        * Death toll = 513
        * Emergency services/hospital staffs all but eliminated
- 250 hospitalized in Boston; 200 in New London; 25 in Durham, NH.
- Outbreaks in several other towns in New Hampshire, Vermont and Massachusetts.

The Predicted Effects

- Immediate
    - 50 infected
    - 35 remain in Hanover
    - Others travel too:
        * Boston (5)
        * New London, NH (5)
        * Football Team (5)
        * Points unknown (?)
- Long Term
    - Hanover:
        * 700 infected by D + 4
        * 7000 infected by D + 6
        * Total infected = 15,715
- Boston
    - 2245 infected
- New London, NH
    - 2245 infected
- Football Team
    - Cancel the season

Disease Transmission Models

- World Health Organization
  - Assumes no treatment or other measures
  - X + X (5) + X (5) (5) + X (5) (5) (5) .
- Johns Hopkins University
  - Assumes public health measure implemented
  - X + X (14) + X (14) (10) + X (14) (10) (2.1)

Notes:

1) X = Number of individuals infected in first generation
2) New X for each geographic area exposed

Treatment

- Streptomycin
- Gentamicin
- Tetracycline
- Chloramphenicol
- Doxycycline
- Oxytetracycline

Prophylaxis

- Tetracycline
- Doxycycline
- Sulfamethoxazole/trimethoprim

"Wild Cards"

- When outbreak is diagnosed as plague
- Start of medical treatment and prophylaxis
- Recognition of symptoms by infected
- Availability of antibiotics
- Ability to provide medical treatment
- Movement of people

The Good News

The terrorist died on September 25th!

Uganda’s Ebola Outbreak, August-December 2000

Adam Geibel

On October 12th, 2000, Professor Francis Omaswa, the Ugandan Director General of Health Services, reported that 30 people had died of a strange disease in Gulu district over the two preceding weeks. This was the first of what would be many accounts of Uganda s Ebola outbreak. The media reports from that remote region of Africa were often contradictory, but probably no worse than

*

Omaswa admitted that the disease had not been diagnosed at that point, but the symptoms (which included high fever, severe muscle pains and bleeding from the mouth, nose and anus) pointed toward Marburg or Ebola virus . He appealed for calm as the investigations continued, but advised people to observe strict hygiene and use gloves and masks when handling infected victims.

An Ugandan Ministry of Health press release said that a total of 42 cases of the disease had been reported, most of them from the village of Rwot-obillo in Aswa county (northern Gulu District). Other cases would be reported in Kasubi and Kabedo Opong (in Gulu).

Samples for testing were flown to the Centers for Disease Control (CDC, in Atlanta) and the high-security National Institute of Virology laboratory in South Africa by the 12th.

Gulu s Population

Gulu is about 270 km (or 180 miles) north of the Ugandan capital Kampala, and had an approximate population of 43,000 in 1993. The market town sits on the crossroads of the main road from Kampala to Sudan and the western route to Democratic Republic of the Congo.

In early 1999, an estimated 80 % of the Gulu county s population was displaced by the 12-year long fighting with the LRA and there were about 400,000 displaced persons across the country s northern border with the Sudan. Most of these were living in 20 crowded camps, unlike the dispersed farms and homesteads surrounded by fields that were the usual settlement pattern in the Gulu and Kitgum countryside.

By 2000, the town was surrounded by small villages with largely illiterate populations, with an estimated total of 150,000. Family "compounds typically found around Gulu are a circle of seven or eight thatched-rood huts, surrounded by corn and cassava fields.

There was also a large Ugandan People’s Defense Force (UDPF) base located nearby, to defend the area against attacks by the rebel "Lord’s Resistance Army" (LRA). The LRA terrorized northern Uganda for 13 years, promising to rule Uganda under guidelines of the Ten Commandments while kidnapping children to turn into small soldiers or sex slaves.

> A nighttime curfew was in effect, since that's when the LRA came to steal children. At dusk, thousands of area residents routinely gathered inside the Lacor Hospital's compound and slept in the corridors. The hospital staff called them "night dwellers."
>
> In the weeks prior to the outbreak, about 15,000 Kenyan herders were driven across the border by a drought

On the 13th, Dr. Crispus Kiyonga, the Minister of Health, Dr. Oladapo Walker, the World Health Organization (WHO) representative in Uganda, Betty Akech, the Gulu Woman MP and state minister for higher education, and an army representative flew to Gulu to join the medical team. They were accompanied by a technical team led by Omaswa.

At that point, one family in Kasubi (near the Gulu UPDF Barracks) had lost seven members to the disease while another family in Kabedo Opong (a Gulu suburb) had lost nine members. One student nurse from Lacor Hospital involved in treating the victims had also died.

That same day, field officials in Gulu told the Ugandan newspaper "New Vision" that at least seven more people had come down with the disease. This brought the number of people affected in the first half of October to 51. At least five patients had been reported to have recovered from the disease at that point, but remained quarantined in area hospitals.

The WHO dispatched two experts to Gulu on the 14th to investigate and advise local health authorities on how to contain the hemorrhagic fever. Protective clothing was also sent to the Gulu area hospitals over the 14-15 October weekend.

On the 15th, Ugandan ministry of health officials confirmed the presence of the disease for the first time in the country. Across Uganda, the MoH started recruiting health education workers to visit affected areas, teach the communities how to prevent the disease and look for new cases. About 200 volunteers were found.

Three of the dead were student nurses from the 500-bed St. Mary's Hospital Lacor; 20-year-old Christine Ajok; 24-year-old Daniel Ayella from Kalongo (east Gulu) and 20-year-old Monica Aol from Kitgum.

Many of the victims had been brought to St. Mary's, which was the best equipped health facility in the area. Two others were seriously ill, while other health care workers in the area admitted to the press that they were scared and tempted to flee. The primitive conditions in these remote African hospitals, as well as practices like reusing scarce needles, meant that the virus was transmitted rapidly in the very places where patients were seeking refuge.

Health officials were terrified that the virus was spread from the infected patients to the "night dwellers", in the weeks before doctors knew the disease was in their midst.

Four Gulu residents died during the day, two from Kanyagoga and two from Kirombe. Unconfirmed rumors were also rampant. A nurse at Lacor Hospital, Achom Christine, told students of Gulu Catholic School that 53 people had died from the hospital while 65 were still under going treatment.

Origin Theories And Misdiagnosis

The area was ripe for epidemics. In addition to a spartan medical network, cultural factors were also working against the Gulu population. Communal eating and washing was commonplace, while polygamy was still practiced and prostitution rampant. Furthermore, HIV has killed hundreds of thousands of Ugandans and infected millions more in the last 20 years.

The Ugandan newspaper "The Monitor" revealed on October 18th quoted Kampala health officials and sources in Gulu that the disease could be traced back as early the first week of August, when a doctor in the Gulu Hospital paediatric ward and another in Lacor Hospital died. Karl Vick of the Washington Post reported on October 20th that a St. Mary's Lacor Hospital physician known as "Doctor Stephen" (in his late twenties and in apparently good health) fell ill with a fever and died two days later, on 8 August. Routine postmortem tissue tests failed to reveal the cause of death.

Health officials thought that those two, along with the death of several other patients, was rather odd. The view among the medics then was that it was some awesomely resistant strain of malaria.

When patients and medics couldn't make sense of the "strange disease" in August and September, fear and superstition took over. The victims relatives began taking most of their dead to witchdoctors, or from the hospitals and simply burying them.

Ugandan mourners would gather in the deceased s hut, keep vigil with the body until the burial (usually the following day). Before sharing food, the mourners skipped washing and dipped their hands into a common bowl to show unity.

But Ugandan authorities initially investigated the death from a mysterious disease of a Congolese woman married to a Ugandan soldier. The South African Press Association reported on October 13th that first victim, who died on September 17, was an unnamed soldier who recently returned from the Democratic Republic of Congo. Gulu district Resident District Commissioner Peter Odok confirmed the deaths and noted that most of the victims lived near the Gulu army barracks.

The Ugandan troops supporting rebels in the neighboring Democratic Republic of Congo since 1998 had recently returned to Gulu, bringing with them Congolese wives. The UDPF withdrew about 4,000 soldiers in the first two weeks of August and about half were sent to camps in Aswa county.

However, on the 14th, Ugandan Health Minister Crispus Kiyonga dismissed these reports during a national broadcast. "Let me point out that the epidemic of Ebola that we have in Gulu District is different from the Viral Hemorrhagic fever recently reported in the DRC. This is because, while this is Ebola, the other one was Marburg. It is therefore evident that this epidemic has not been imported from the DRC."

Kiyonga claimed that all UDPF soldier withdrawn from the DRCongo underwent medical checks before they were released to their barracks and that none were infected with Ebola.

The State Minister for Health, Max Omeda, theorized that LRA rebels could have brought the Ebola fever from their bases in the Sudan. There are thousands of refugees from the Sudan in the area, as well as Sudan People’s Liberation Army (SPLA) rebels who are fighting the Khartoum government.

In a press conference on the 16th, Kiyonga noted that the first Ugandan Ebola case was an unnamed month-old child who had not been in contact with soldiers. The child was from the family that suffered seven deaths due to Ebola.

Ebola History

Ebola is named after a river in the former Zaire (now the Democratic Republic of Congo) where it was first recorded in a number of villages in 1976. Outbreaks were also recorded in 1977.

Ebola, which can spread through contact with bodily fluids, takes between four and 14 days to kill its victims and causes massive internal bleeding, vomiting and diarrhea. However, it is also described as a rapidly progressing disease and can kill within 24 hours. Lethal to 90% of those infected, there is no known cure. Death usually comes when the victim ’’bleeds out’’ through the eyes, nose, ears and other bodily orifices.

Outbreaks were also reported in Sudan in 1976 and 1979, Ivory Coast, Liberia and Gabon in 1996, along with cases of an Ebola-like virus in monkeys in the United States in 1996.

The 1995 Ebola outbreak killed 245 people in Kikwit, in the Democratic Republic of Congo. (Kikwit had a population of 400,000 and is 400 kilometers east of Kinshasa, the capital of DR Congo.)

The last recorded Ebola outbreak was in Gabon in February 1997, which killed 10 people. Of the 1,100 cases recognized by the WHO since 1996, 793 people have died from Ebola.

Authorities in Uganda have been preparing since 1998 for an outbreak of viral hemorrhagic fever (VHF)*. Osama told the French newswire AFP that "We already have guidelines in place to deal with a disease of this kind. We’ve had a multi-sectoral National Task Force on Viral Hemorrhagic fevers in place for two years. We knew that there had been outbreaks of Marburg, which is another VHF, in areas of (DR) Congo near the Ugandan border, so we have had our eyes on the eight districts bordering Congo."

* Ugandan doctors attributed the response to a culture that places emphasis on health and education. Uganda was home to the first medical school in East Africa and is the only African country that has slowed HIV infection rates. The emphasis on reducing HIV - another virus carried in bodily fluids - prepared the Ugandans for Ebola.

Esther Awete

The Associated Press quoted Gulu district health officer Okat Lokach s claim on October 17th that local officials traced the disease to an unnamed housewife who died September 17th. The next two victims were her daughter and mother. Other mourners returned to their villages, became ill and infected friends and family. The first of these victims reached a hospital on October 7th.

In wasn t until October 18th that Associated Press reporter Chris Tomlinson wrote that 36 year old Esther Awete was found dead five days after she fell ill with a fever. At first, her neighbors thought Awete had died from dysentery, cholera or one of the other common illnesses found in the area.

Her body was kept in her hut for two days, so that friends and family could take part in the funeral. On September 17th*, Awete’s family and closest friends ritually bathed her body, buried her less than 30 feet from where she died and then washed their hands in a communal basin as a sign of unity.

One of Awete’s two children, a 9-month-old boy, died of Ebola within days of her funeral. Her mother, three sisters and three other relatives also died, though her 8 year old son (who was not at the funeral) survived.

*Originally misreported in the AP article as the 27th

Quarantine Failure

While Ugandan authorities told Reuters on October 16th that although they believed the situation was nearly under control, three areas where the majority of cases originated were placed under quarantine (Bugantira, Aswa county and Pece and Bardege, both in Gulu municipality).

Lieutenant-Colonel Walter Ochoro, Gulu district chairman of a disease task force, told the press that said "We hope we will not have to use force but we are determined to beat this."

All schools in the affected areas had been ordered closed and residents were told they could not leave except for medical attention. Local radio advised people not to shake hands, share plates or cups, and to stay in their homes.

The medical staff at hospitals in and around Gulu were overwhelmed by the virulence of the disease while WHO figured that the provisional death toll was 43 (WHO s 16 October press release stuck to the figure of 35 dead, with 71 infected). The Gulu hospital alone had 26 patients.

However, quarantine measures were not apparently entirely effective. By the morning of the 16th, there were 73 documented Ebola cases in the north of the country. Two of these were reported in St. Joseph's Hospital in Kitgum. One of the student nurses who died in Lacor Hospital after treating Ebola patients was buried in Kitgum.

Mike Ryan, the WHO disease outbreak coordinator, said that it was not necessary for Uganda to impose travel restrictions to or from the area. Ryan told the press that "Cordoning off an area does not work in situations like this. Travel restrictions would be inappropriate because the disease is in a very remote part of Uganda and it spreads with direct contact with bodily fluids, not by sitting next to an ill person on a plane. This disease is controllable, it is containable. But slapping on measures of restricting movement is not going to be effective, particularly when it comes to international travel. Such steps are rarely effective and could backfire by damaging the local economy, thereby indirectly hurting the population's health."

Kenyan health authorities sent a medical team to Busia (the main border crossing point between Uganda and Kenya) on the 16th, to identify and isolate suspected Ebola cases. Since thousands of people cross the border at Busia every day suffering from other endemic illnesses (such as malaria and AIDS-related diseases), the Kenyans would have a difficult time finding infected travelers. Furthermore, at least one busload of Ugandan travellers entered Kenya without an inspection after the medical team had arrived on site.

Authorities in Rwanda and Tanzania had also stepped up border checks. Meanwhile, the British High Commission and the US Embassy in Kampala advised their citizens against travelling to Gulu following the outbreak.

The Ugandan daily newspaper "The Monitor" said that employees of the Norwegian Refugee Council (NRC), Action Contre la Faim, Catholic Relief Service and International Organization for Migration had left Gulu. Gulu's secretary for health, Betty Ochan, told the newspaper that the NGO officials had temporarily relocated to Kampala. Officials from Red Barnet, Save the Children-Denmark and International Committee of the Red Cross had reportedly packed their bags as well.

Traffic between Gulu and Kampala was reported to have remained normal. The "New Vision" noted passengers and businessmen disembarking at the bus and taxi parks, while Kampala wheelbarrow pushers were not scared to interact with passengers from Gulu.

A Reuters correspondent reported that while people in most places were observing the quarantine, a packed minibus left Gulu for Kampala on the 17th. Colonel Ochoro told the press that "we are just advising people to stay where they are. But we are not using roadblocks or anything like that. We just have to hope they follow our advice."

Another sign of panic might have occurred at Lira Hospital, after John Awio (from Alito in Apac) was admitted over the 14-15 October weekend with suspected symptoms (a bleeding nose) was snatched from one of the wards. He disappeared the night of the 15th, after his condition worsened.

Dr. Fred Nyangkori, the hospital s Acting Medical Superintendent, confirmed the event but noted that they were still investigating the patient's removal and could not depend on the report of the nurse.

Opwonya Ayubi, headmaster of the Gulu Prison Primary School, admitted that his facility closed at 9:30 AM on the 17th. Yoti Zabulon, a senior doctor on the Ebola ward at St. Mary's Hospital, noted that four cases had come in on the 16th and one early on the 17th.

Two more patients died on the 17th, which Reuters reported brought the Ugandan government's official death toll to 39 people. An unnamed health ministry statement said that the death toll was still at 35. He added that the number of infected people had risen to 81, 46 of whom either recovered or were still ill.

In Gulu, health officials were conducting house-to-house searches for infected persons and were quarantining anyone complaining of flu-like symptoms, diarrhea or vomiting. Anyone found with early symptoms of the disease was quarantined and counted as a potential victim.

Omaswa admitted that the searches might result in the discovery of more infected people, but that this was to be expected and that people should not be alarmed. Local radio announced that all Ebola victims who died were to be buried by the police, army or prison officers. Shaking hands was forbidden.

Cases were also reported in the Amoru, Pabbo, Parabongo and Atiak refugee camps, all in Kilak county west of Gulu town. Rumors began to spread of cases in other districts of Uganda, which could be interpreted as a spread of the disease or just panic.

Dr Matthew Lukwiya, medical superintendent at St Mary's Hospital, said no new deaths had been reported at his facility. Four people were reported to be in critical condition during the day, and at least six cases were reported from the displaced persons camps.

The World's Initial Response

Uganda officially requested the world's assistance on the 16th. By then the CDC, Department for International Development (DFID) of Britain, the WHO, UNICEF, the French Doctors Without Borders (MSF) and the International Committee of the Red Cross were the first to provide over $400,000 aid.

The DFID donated $ 280,000 and CDC provided technical assistance, while the WHO offered $ 60,000 and five technical experts (two of whom were already in Gulu).

World Vision provided the ministry with ground staff, UNICEF donated a vehicle and $ 60,000, France's MSF offered eight technical assistants, protective wear and a vehicle, while the International Committee of Red Cross (ICRC) donated protective supplies.

When the Ugandan Ministry of Health established a National Task Force for the Control of Viral Haemorrhagic Fevers, WHO supported this by;

* coordinating the international response to the outbreak,
* implementing disease control measures, such as
    - A) barrier nursing procedures,
    - B) case finding,
    - C) contact tracing and monitoring,
    - D) supplying protective equipment.

Tables 1 and 2 below were compiled by Epidemiological Surveillance Division, Ministry of Health, Kampala Uganda.

TABLE OF DISTRIBUTION OF CASES BY AGE-GROUP: 16 OCTOBER 2000

Age Group	Frequency	Percentage
Cases less than 1 year	7	15.9
1-9 years	4	9.1
10-14 years	1	2.3
15 years +	32	72.7
Total	44	100

TABLE OF DISTRIBUTION OF CASES BY VILLAGE: 16 OCTOBER 2000

Village	Frequency	Percentage
Rwot-Obilo	16	37.2
Kabedo-Opong	9	20.9
Kasubi	8	18.6
Lacor Nurses School	5	11.6
Kony Paco	2	4.7
Ariaga	1	2.3
Pece Pawel	1	2.3
Water Quarters	1	2.3
Total	43	100

A three-man, Geneva-based World Health Organization team with eight boxes of protective gear (including gowns, gloves, masks and boots) arrived in Kampala on the 17th and were to leave for northern Uganda two days later. These supplies, particularly masks, were in critically short supply and local seamstresses had started sewing cloth ones.

Led by the Director of the Department of Communicable Diseases and Surveillance Response, Dr. Guenael Rodier, Dr. Michael Ryan and Dr. Simon Mardel, would train and work with Ugandan health workers. Ryan and Mardel participated in responses to similar epidemics in the DRCongo (formerly Zaire) and Gabon.

Rodier wanted to monitor anyone who come in contact with Ebola patients or their bodies for three weeks, which was the maximum incubation period. He thought that 100 to 200 people could be incubating the disease.

*

On the 18th, Omaswa noted that there were 10 new cases over the previous 24 hours. Four were admitted to Lacor hospital and six to Gulu hospital. The last admission was on the morning of the 17th. Omaswa said the cumulative number of infected people stood at 94. While there were no deaths reported for the previous two days (the 16th and 17th), there were four deaths during the previous 24 hours.

By then, 80% of the cases had been reported from three sub-counties Bar Dege (30%); Bungatira (28%); and Pece (15%). All, with the exception of part of Pece, were in Acwa County.

The UN s. World Food Program, already active among the northern Ugandan refugee population, was delivering food to hospitals treating victims. Non-governmental agencies and volunteers committed themselves to continue working in the face of the crisis.

Positive Identification

A total of 111 cases had been reported by 8 AM on the 19th, when the leader of a U.S. Centers for Disease Control team, Pierre Rollin, announced that the virus was Ebola Sudan. At least 41 people had died, said Okat Lokach, the Gulu district health director.

Four CDC epidemiologists and two microbiologists arrived in Kampala with laboratory equipment. They would separate those who were infected from those with similar symptoms, in an attempt to determine the source of the outbreak.

On the 20th, WHO launched an international appeal for $848,000 to help the Ugandan government and Ugandan authorities allocated $200,000 to fight the outbreak. On that day, 47 had died and 122 cases had been reported.

That day, the most affected areas include Rwot Obilo in Aswa County, Kabedo Opong, Kasubi and Kirombe from the Gulu town Municipality. Preliminary reports indicated that some of the risk factors that may have contributed to the spread of the disease before the isolation and barrier nursing techniques were put in place were caring for the sick and participating in the burial of the dead. This would account for the abnormally high rate of females over 15 who were felled by the disease.

Tables 1 and 2 below were compiled by Epidemiological Surveillance Division, Ministry of Health, Kampala Uganda.

TABLE 1: DISTRIBUTION OF CASES BY AGE-GROUP - 20 OCTOBER 2000

Age Group	Frequency	Percentage
Cases less than 1 year	9	7.4
1-9 years	9	7.4
10-14 years	7	5.7
15 years	+97	79.5
Total	122	100

TABLE 2: DISTRIBUTION OF EBOLA CASES BY TYPE OF WORK -20 OCTOBER 2000

Ocuppation	Cases	Percentage
Babysitter	1	0.8
Carpenter	2	1.6
Driver	1	0.8
Housewife	48	39.3
Local Police	1	0.8
LCI Official	1	0.8
Nurse	2	1.6
Peasant Farmer	21	17.2
Porter	1	0.8
RTD Chief	1	0.8
Student/Pupil	21	17.2
Teacher	2	1.6
Not Employed	20	16.4
Total	122	100.0

TABLE OF DISTRIBUTION OF CASES BY OCCUPATION - 20 OCTOBER 2000

Occupation	Frequency	Percentage
Housewife	16	36.36
Peasant	9	20.45
Children	6	13.64
Student Nurses	5	11.36
Pupil	2	4.55
Baby Sitter	1	2.27
Baby/Neonate	4	9.1
Local Police	1	2.27
Total	44	100.0

Spreading Terror

By the 21-22 October weekend, at least 51 had died and 139 were reportedly infected. While Ugandan officials in Gulu insisted the worst was behind them, others were less optimistic. WHO spokesman Valary Abramov said it was much too early to predict when the outbreak would reach its peak. Dr. Sam Zaramba, director of health services in Uganda, told reporters that an estimated 200 people had come in contact with Ebola victims.

On the 22nd, Omaswa said three people had died in the previous 24 hours and ten new cases had been identified in the same period. The next day, Okware said that 11 new cases were identified in the previous
24 hours but the first time in more than a week, the Ebola death toll had not increased during that time period.

Traditionally, relatives helped care for patients and feed them, but the possibility of the disease spreading in this way was too great to permit the practice to continue. In an effort to prevent the spread of the disease, two burial sites were set aside for Ebola victims near Gulu's two hospitals.

In Kenya, a woman was admitted to the Naivasha District Hospital (37km from Nairobi) on the morning of the 23rd and her symptoms were mistaken for Ebola. A medical team from Afya House and the Kenya Medical Research Institute was sent the next day to investigate. The week before, there were two hoaxes at the Kenyatta National Hospital including one of a patient who arrived from Bukavu in the Democratic Republic of the Congo with a high fever.

Kenyan police sealed four illegal cross-border routes into Uganda on the 26th, leaving only the main Busia and other major posts. Police officers were to prevent the entry of persons untested for the disease.

Another route across the Lwakhaka river was closed due to heavy rains, which made the river impassable.

The Mt Elgon district public health officer, Paminas Kathinja, said that Ugandan visitors had to report to the Chekube government dispensary before being allowed entry to Kenya. One of the entry conditions at the legal border posts was that travellers from Uganda fill out an Ebola form, declaring their state of health.

At the Ministry of Health headquarters in Kampala, Okware told journalists that 10 new patients were admitted between 8.00a.m on the 24th and 8.00a.m on the 25th, which brought the total number of cases to 175.

The Kampala newspaper "The Monitor" editorialized that the capital city was ripe for it s own wave of Ebola. Director of Health Services Dr. Misaki Mubiru claimed that over 70% of the diseases in the city were related to the lack of sanitation. The city flooded when it rained, sewage regularly sprung from alleys onto the pavements and across streets. Garbage heaps punctuated the city and old or war-ruined buildings provided numerous homes for rodents.

The paper recommended a quarantine in the Mengo-Kisenyi, Kalerwe-Kibbe, Kireka-Kamuli, Naguru go-down, Kasubi-Nabulagala and Kajjansi-Kawuto neighborhoods. They also suggested that the brunt of a quarantine initiative should be directed to city s numerous food sellers, who posed a constant sanitation threat.

The Army And Disease In The South

A 20 year-old UDPF soldier, Samuel Bandese, was infected when he traveled from his base in Gulu to to his home town of Mbarara to visit his ailing father. The soldier was brought to Mbarara hospital on 22 October in an army lorry and his death on 27 October was the first confirmed Ebola case outside of northern Uganda s Gulu district.

While Bandese had been in the DRCongo with the UDPF s 57th Battalion in 1997, he returned to Uganda around 1998 and relocated to Gulu. Since the incubation period of Ebola is 21 days, there is no way he could have contracted the disease in Congo.

A team from the health ministry was dispatched to Mbarara and the health ministry joined with the army in order to track down any soldiers who might have come into contact with Kabango before he died. The busy commercial town of Mbarara, about 425km (265 miles) south of Gulu, is the headquarters for all western Ugandan military activities.

Two people who came into contact Kabango were admitted to the Mbarara ebola ward - one of whom was 27-year-old Geoffrey Kabango, a prisoner on parole looking after sick prison inmates and soldiers in Mbarara University Hospital.

Two versions of the story were published. One was that Kabango was attending to Bandese and shared a bed with him. The other was that Bandese became crazy the night before he died and forced his way into bed with the prisoner. Whatever the facts, Kabango later developed a fever and chest pains.

The second patient, who was hospitalized in Mbarara on 3 November, had also come in contact with the prisoner.

On the 2nd, Mulago Hospital admitted a UDPF soldier named Busheija with a fever in the afternoon and isolated for monitoring in the White House by Dr. Zati. Ag. He had attended the burial of an Ebola victim in Mbarara on the 27th. Relatives rushed him to Mulago, suspecting he had the dreaded Ebola virus.

On the 4th, Sam Okware noted that 15 doctors, nurses and sweepers who worked in the ward where the sick man was held were being closely watched for Ebola symptoms. Okware also said that the feared Ebola case in Mulago was confirmed false and the person buried in Mbarara was not an Ebola victim.

"Another soldier (Busheija), left Kampala and died mysteriously in Sanga (12 miles from Mbarara), after suffering from diarrhoea and vomiting blood. Those who went for the burial came back complaining and they were isolated. But that case wasn't Ebola, the soldier was suffering from gastroenteritis,"

Uganda's Ministry of Health called on the military to restrict the movement of soldiers from the northern district of Gulu. The Ugandan Army was alarmed enough by the epidemic to requisition supplies of gloves, detergents and other protective gear from the Ministry of Health, as well as dispatch teams of investigators to trace the movements of Private Bandese.

The third UPDF soldier, Brahamin Esatume 30, died in Mbarara University Hospital at 7:00 am on the 9th.

The Rising Toll In The North

The Catholic church s medical missions were especially hard-hit. Two professional nurses died: 42-year-old Margaret Adota, who worked as a stretcher bearer, that left behind 10 children; and Florence, mother of one. Other nurses who survived the infection were 26-year-old Sister Helen Alobo of the diocese of Lira (south-east of Gulu); 18-year old Irar Irene, a student of the nurses school; and 20-year-old Aber Sharon. Around 23.30 on 5 November, 45 year-old Sister Pierina Asienzo of the Little Sisters of Mary Immaculate died from Ebola in Gulu s the government hospital

The WHO supplied the Gulu district with 20 walkie-talkies on 6 November, to increase communications and supplement the purchase of three mobile phones.

Six new cases were admitted in Gulu and Mbarara reported no new cases on the 10th, while another was discharged from a Gulu Hospital.

Ebola cases in Gulu dropped to zero new casualties on the 13th. However, early in the morning, 60-year old Gideon Alwala, died from Ebola in Kiryandongo Hospital along the

Kampala-Gulu highway. Alwala was also a relative to the first three Kaduka (Masindi Port) residents who died of Ebola.

The United States Department of State warned Americans to stay away from funerals in Uganda on the 15th. That same day, the NGOs reported that no new Ebola patients had been detected anywhere in the country for three days, despite a door-to-door search by scouts. The Task Force meetings were reduced to two a week (on Tuesdays and Fridays). Press briefings were also reduced to twice a week, or more if the need arose.

> The problems didn t end with patient s discharge. James Akena, a 40-year old Gulu town resident who lived alone, was admitted to a hospital on 21 October and tested positive for Ebola, but was cured and released on the 30th. After being discharged from the hospital, a nurse accompanied him home. They found Akena s house and all his belongings burned, then his neighbors chased the two away. The homeless and broke Akena spent several days without food in an outdoor bus station, until case workers discovered him.
>
> The first to be shunned were the Ugandan soldiers, but then the stigmata of the disease moved from the UDPF troops to those related to the victims. At one funeral, mourners undressed and abandoned their clothes at the graveside, thinking they might be infected.

Spreading Disease Outside of Gulu

Ebola was carried to Masindi by Hellen Okwisa, a patient at Lacor hospital who had been admitted with ascites (water in the abdomen). When she discovered that there were Ebola cases in Lacor, she fled to her home near Masindi (Masindi Port is on the Nile River, 99 miles south of Gulu). Okwisa died on October 25th and was buried two days later. A child in the same household died soon afterwards, followed by Okwisa’s own daughter and then her daughter’s husband.

For two weeks, health officials were ignorant of these new cases. Then, on 13 November, Medecins sans frontieres (MSF) confirmed the outbreak of Ebola fever after a team was sent to Kiryandongo in Masindi district (180 km northwest of Kampala) to assist in containing the new outbreak. Two staff members helped set up an isolation ward, after the two people died from Ebola symptoms and a third person tested positive for the disease. Of the 73 patients in Masindi district s Kiryandongo Hospital, 33 fled the hospital without permission, in fear of contracting Ebola.

Health officials in Uganda tried to find anyone who had direct contact with the woman - including those who helped bury her. The 150 residents who attended the burials in Masindi Port of three recent Ebola victims - all relatives. The husband of one of the three, who was also from Masindi, later died of Ebola as well and was buried in the cemetery of the hospital, in Kiryandongo, 133 miles north of Kampala, to prevent further spreading of the virus.

They warned the Kenyan Health Ministry that seven Kenyans were among 150 people that Ugandan authorities believed might have come into contact with the disease at funerals for three Ebola victims. Senior Kenyan health officials held a meeting on the afternoon of the 14th, while the seven Kenyan mourners were traced and quarantined in their homes.

They were from Yuodat village in the Mt.Elgon region, Nambala in Busia and Kitale Transoia area. All of them showed no signs of Ebola by the 15th, but were to be monitored for 42 days before they would be declared free of infection.

Over 20,000 people crossing the Kenyan-Ugandan border since the Ebola outbreak started had been screened and no cases of the virus had been found. However, authorities made no mention of travelers who avoided any border checkpoints.

Kenyan radio reported on the 10th that direct flights between the northern town of Lokichokio and Gulu in northern Uganda had been suspended to check against the spread of Ebola. Lokichokio Ebola surveillance coordinator, Dr Geoffrey Kasembeli, said the move was aimed at restricting the inflow of people from Ebola-stricken areas of Uganda. No case of the epidemic has however been reported in Lokichokio and its environs.

Belgium also initiated screening precautions. On 10 November, passengers aboard a Brussels-bound Sabena Airlines flight from Entebbe via Nairobi were required to fill out forms presented by the Belgian immigration officers 30 minutes before the plane landed.

The form, printed in English, Flemish and French, required passengers to indicate their places of departure from Uganda, place of residence in Belgium, street and phone numbers, as well as their arrival date in the country and flight seat numbers. The form explained that "Following the outbreak of the epidemic of hemorrhagic fever Ebola, it's necessary for each traveller returning from Uganda to fill out this form. This information will be treated as strictly confidential."

Doctor Walter Kayawaya of western Kenya s Busia District Hospital said that the hospital had confined George Ekokwa on the 15th, after he fell ill following his return from Uganda the week prior. National disease control chief Dr. Alex Opio said that samples of Ekokwa s blood had been flown to Gulu, where the WHO and CDC would test it for Ebola in their mobile laboratory.

Back in the Masindi district, Ebola task force chairman John Majara said that the Ebola treatment center would be transferred from the Kiryandongo Hospital (only eight km from the Ebola outbreak) to Masindi hospital, 50 kms away. The Kiryandongo hospital lacked a reliable power supply, running water and communication facilities.

In Tanzania, 47-year old Dar es Salaam resident Ramadhan Omar was admitted to Muhimbili National Hospital on 17 November. The Gongo la Mboto resident showed all of the classic Ebola symptoms and was said to be either a truck driver or businessman who traveled between Tanzania and Uganda.

A recently-admitted, unnamed patient suspected of being from a neighboring country died at Bugando hospital in Mwanza (in northern Tanzania, on southern shore of Lake Victoria). The Director of Bugando Medical Centre, Dr Samson Winani, said that the deceased had shown all signs of having contracted Ebola and specimen taken from him had been sent to South Africa for verification. The patient had been brought to hospital by a taxi driver, who had picked him at the central bus stand.

Specimens had been taken from both men and sent to South Africa for verification.

When Would It End?

After 42 days (or two incubation periods) without admissions in the hospitals, Uganda would finally be declared Ebola-free.

Attachments
Affected Villages Graph, 9 November 00

Uganda's Ebola Timeline

Date	Cases	Dead	Recovered	
8 Aug	?	1	?	"Dr. Stephen"
17 Sep	?	2	?	Esther Awete
21 Sep	?	4	?	
23 Sep	?	5	?	
29 Sep	?	6	?	
2 Oct	?	8	?	
4 Oct	?	9	?	
6 Oct	?	13	?	
7 Oct	?	17	?	"First" victim reaches a hospital
8 Oct	?	-	?	
9 Oct	?	18	?	
10 Oct	?	20		
11 Oct	?	21	?	Ugandan Health Ministry Figures as of 16 October
12 Oct	42	30	?	
13 Oct	44	27/30	?	Case Fatality Rate (CFR) 61% (for 27 deaths)
14 Oct	51	31	?	Disease identified as Ebola
15 Oct	63	31/33	5	CFR 52.4% for 33 dead/Three Lacor Hospital nurses die
16 Oct	71/73	35/43	?	CFR 52.4% for 35 dead/Conflicting figures between gov. &WHO
17 Oct	81	35		?
18 Oct	94	39	?	Francis Omaswa figures
19 Oct	70	41	?	Disease specifically identified as Ebola-Sudan
20 Oct	149/160	54	?	Dr. Sam Okware/ Francis Omaswa figures
21 Oct	122	47	?	CFR 38.52%
22 Oct	139	51		?
23 Oct	160	54		?
24 Oct	165	60		25?
25 Oct	175	63/64		57
26 Oct	182	64	-	No deaths in previous 24 hours
27 Oct	191	67/68	73/75	
28 Oct	205	71	75	CFR 35.6%
30 Oct	224	73	96	CFR 32.6%
31 Oct	239	75		107
1 Nov	250	80	117	

2 Nov	262	81	134	CFR 30.9%
3 Nov	265	83	141	
4 Nov	267/269	84/87	148/149	2nd set of figures from Okware. CFR 36%
6 Nov	280/281	89/91	155	
7 Nov	284	91	166	No deaths in preceding 24 hours.
8 Nov	288	96	?	
9 Nov				
10 Nov	300	100	171	
11 Nov	306	103/105	172/183	Figure change occurred during day.
12 Nov	320	102		
13 Nov	323	110	191	Kenyans tracked, quarantined
15 Nov	320/336	105/117		Ugandan M.o.H. figures for Gulu/Press figures
17 Nov	322/331	107/115	206	Ugandan M.o.H. figures for Gulu/Press figures

For Additional Reading

Viral Hemorrhagic Fevers: Fact Sheets Ebola Hemorrhagic Fever
http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.htm

Ebola Virus Hemorrhagic Fever: General Information (Circa 1995)
http://www.cdc.gov/ncidod/publications/brochures/ebolainf.htm

WHO - EBOLA HAEMORRHAGIC FEVER Fact Sheet 103 (Revised September 1997)
http://www.who.int/inf-fs/en/fact103.html

NEW VISION - Ugandan Daily Newspaper
http://www.newvision.co.ug/

References

Militias Sign Up To Defend Villagers, Jennifer Bakyawa, IPS, 28 Apr 99
Strange disease kills 30 in Gulu, Charles Wendo, New Vision, 13 Oct 00
Mystery Fever Kills 40 in Uganda, SAPA-AFP, 13 Oct 00

Ebola Virus Reported in Northern Uganda, PANA, 15 Oct 00
Ebola Outbreaks In Northern Uganda, HENRY WASSWA, AP, 15 Oct 00
Uganda long prepared for outbreak of hemorrhagic fever, AFP, 15 Oct 00
Ebola Virus Reported in Northern Uganda, PANA, 15 Oct 00
Ugandans Slap Quarantine on Ebola Virus Areas, Gavin Pattison, Reuters, 16 Oct 00
Uganda Appeals for International Help to Tackle Ebola, PANA, 16 Oct 00
Ebola haemorrhagic fever in Uganda, WHO Press Release, 16 October 2000

Uganda Doctors Report New Ebola Virus Cases, Paul Busharizi, Reuters, 17 Oct 00
Ebola now hits Kitgum, New Vision, 17 Oct 00
US, UK warn on Gulu travel, New Vision, 17 Oct 00
Gulu traffic normal , New Vision, 17 Oct 00
WHO against flight restrictions on Uganda, New Vision, 17 Oct 00
Deadly Ebola Now Spreads to Kitgum, 73 Infected, Carolyne Nakazibwe, The Monitor, 17 Oct 00

Ebola Fever Panic Grips Northern Uganda, PANA, 17 Oct 00
Uganda's Gulu Town a Haven for Ebola Outbreak, Gavin Pattison, Reuters, 17 Oct 00
NGOs flee Ebola stricken North, William Tayeebwa and Oketch Bitek, The Monitor, 17 Oct 00
Residents flee Ebola patients, David Kibirige, Lucy Lapoti & Hudson Apunyo, The Monitor, 17 Oct 00
Where Disease and War Intersect, Karl Vick, Washington Post, 17 Oct 00

Ebola Cases Expected to Rise in Northern Uganda, Gavin Pattison, Reuters, October 18, 2000
Ebola experts rush to Lira, Charles Wendo, New Vision, 18 Oct 00
WHO flies in equipment, New Vision, 18 Oct 00
Medical Supplies Run Short in Uganda, Chris Tomlinson, AP, 18 Oct 00
Source of Ugandan Ebola Found, Chris Tomlinson, AP, 18 Oct 00
Ebola 'Spreads' to Soroti, Lira, Atiak, Oketch Bitek And Patrick Elobu Angonu, The Monitor, 18 Oct 00
Health Workers Search For Ebola Victims, PANA, 18 Oct 00
Lesson From Ebola; We Need Law for Burning Bodies, The Monitor, October 18, 2000
Organised Response Needed Over Ebola, The Nation, October 18, 2000
Health Workers Search For Ebola Victims, PANA,October 18, 2000
Ugandan authorities search for frightened victims of Ebola outbreak, AP, 18 Oct 00

Experts Help Tackle Ebola Outbreak, More Than Three Dozen Die in Uganda, Chris Tomlinson, AP, 19 Oct 00
WFP Continues Giving Food in Ebola Area of Northern Uganda, PANA, October 19, 2000
Ugandan Ministry Of Health Press Release - Updates on the Ebola outbreak, 19 Oct 00 Morning Edition
Ebola Probe Looks Further Back, Karl Vick, Washington Post, 20 Oct 00
Ugandan Ministry Of Health: Trends on the Ebola outbreak, 20 Oct 00
Uganda in terror as ebola spreads , Wanyama Wangah, The Sunday Times, 22 Oct 00
Ebola Virus Death Toll Climbs to 54, Henry Wasswa, AP, 22 Oct 00
Ebola Death Toll Remains Stable, Henry Wasswa, AP, 23 Oct 00
WHO Says Deadly Ebola Outbreak to Last Months, Reuters, 24 Oct 00
Death Toll in Ebola Outbreak Climbs, AP, 24 Oct 00
Watch MPs When Ebola Comes to Kampala, Vincent E. Bua, The Monitor, 24 Oct 00

Ebola Scare in Naivasha, The Nation, 25 Oct 00
Kenya Seals Border Routes With Uganda to Contain Ebola, Tervil Okoko, PANA, 26 Oct 00
33 People Recover From Deadly Ebola Virus, New Vision, 26 Oct 00

Ebola Virus Spreads South, UN Integrated Regional Information Network, 2 Nov 00
Ebola spreads to south west Uganda, BBC, 2 Nov 00
Officials suspect new Ebola case in south Uganda, Reuters, 3 Nov 00
Mbarara Ebola Man in Mulago, Carolyne Nakazibwe, The Monitor, 3 Nov 00
Ebola Spreads From Northern To Southwestern Uganda, Sapa-AFP, 4 Nov 00
15 Ebola Suspects in Mbarara Hospital, Carolyne Nakazibwe, The Monitor, 4 Nov 2000
Ebola Kills Sister Pierina, Martyr of Charity, MISNA, 6 Nov 2000
Army Factor in Ebola Outbreak, David Kaiza and A. Mutumba Lule, THE EAST AFRICAN, 6 Nov 00
Ugandan Ministry Of Health Press Release - Updates on the Ebola outbreak, 7 Nov 2000
Ugandan Ministry Of Health Press Release - Updates on the Ebola outbreak, 9 Nov 00
Uganda Ebola Toll Reaches 103, Survivors Shunned, Reuters, 10 Nov 00
Mbarara Soldiers Ebola Deaths Reach Three, Carolyne Nakazibwe and Arinaitwe Rugyendo, The Monitor, 10 Nov 00
Government To Assist Ebola Victims, Carolyne Nakazibwe, The Monitor, 11 Nov 00

Ebola Virus in Uganda Kills 105, AP, 11 Nov 00
Ebola Spreads to Third District, UN Integrated Regional Information Network, 13 Nov 00
Ebola Outbreak Linked to Woman, Henry Wasswa, AP, 13 Nov 00
Uganda warns Kenya Ebola could have crossed border, Reuters, 14 Nov 00
Fourth Ebola Victim Dies in Masindi, Carolyne Nakazibwe, The Monitor, 14 Nov 00
Uganda Warns Kenyans on Ebola, Henry Wasswa, AP, 15 Nov 00
Kenyan hospital isolates man amid Ebola fear, Reuters, 15 Nov 00
U.S. warns Americans of Ebola risk in Uganda, Reuters, 15 Nov 00
30 Patients Flee Kiryandongo Over Ebola, New Vision, 16 Nov 00
No new Ebola cases reported, Carolyne Nakazibwe, The Monitor, 16 Nov 00
Belgium screens Ugandans for Ebola, Robert Mugagga, The Monitor, 16 Nov 00
Ebola claims three more, Charles Wendo and Kyetume Kasanga, New Vision, 16 Nov 00
Ebola survivors face fear and rejection in Uganda, AP, 17 Nov 00
Ugandan Ministry Of Health Press Release - Updates on the Ebola outbreak, 17 Nov 00
Kenya brings blood for Ebola virus tests, Charles Wendo, New Vision, 18 Nov 00
Tanzania gripped by fear of ebola epidemic, two suspected carriers tested, The Guardian, 20 Nov 00

The Hanover Virus of 2005

Adam Geibel

Outbreak. Plague. Virus. To the layman, those terms were interchangeable in the Fall of 2005. They all described the first biological warfare attack on Homeland America.

Only months after the crisis was over did it become known as The Hanover Virus.

WHO LET THE GENNI OUT OF THE BOTTLE? The People s Democratic Republic of Krasnovia

The People s Democratic Republic of Krasnovia is a fictional desert country, based on the former southern Soviet Republics. Krasnovia s leadership is hostile to America but her military forces are far weaker and pose no conventional threat to America. This creation was used by the American military as a generic opponent, specifically for operations at the National Training Center at Fort Irwin, California.

The following scenario is a work of fiction, but illustrates what could very well happen in the real world.

*

The White House had a long history of problems with the People s Democratic Republic of Krasnovia, spanning more than a decade and three Washington administrations. Despite heavy shuttle diplomacy throughout 2004, tensions rose after Christmas of that year.

Economic sanctions by the United States and the European Union were instituted in January, followed by a a blockade in March. The Krasnovians had decided they had had enough of the US/NATO embargo by mid-2005.

On 4 July 2005, agents of the Krasnovian government in an unnamed Mideastern city met with Ahmed, a little-known but combat-proven Mujihadeen of the great Jihad. The growing tension between Krasnovia and her neighbors, Parumphia and Mojave, was reaching the boiling point but Krasnovia s military was nowhere near strong enough to seriously threaten the Mojavians ally, America.

But that situation was about to change.

Near the end of his meeting with Krasnovia s unnamed friends and supporters, Ahmed was given four things — a Cayman Islands bank account number, verbal instructions and the blessings of the Krasnovian people. The last item was a toiletries kit. In it was an aerosol can of deodorant and another of shaving cream, as well as the usual toothbrush, razors, etc.

His leaders carefully, gleefully explained that the two aerosol cans were actually dispensers for a substance that had originated in the Sergiyev Posad Biowarfare lab of the old Soviet Union, a very lethal biological agent that had been experimented with as a potential weapon.

In a side pocket of the toiletries case were four brushed aluminum cigar cases, each holding a pencil-thin sealed vial filled with same substance.

Since the blockade of Krasnovia had hurt her children, since America s support of the Zionist government hurt Palestinian children, since American funds transferred to the Mojave government had hurt Parumphian children, it had been decided that America s children would be the first target.

*

THE EXECUTIONER

Ahmed left the meeting at dawn to a chorus of sa lams from the Krasnovians. This would be the crowning battle of his personal Jihad — to carry the fight to the heart of the Great Satan itself.

Born in 1964, Ahmed s parents were Krasnovia. They had left before that country was torn apart by civil war and were able to secure homes in Canada. Ahmed grew up fairly comfortably in that mosaic society and was in his first year at the University of Toronto when the Jihad called him.

The Soviet Bear was deep into Afghanistan in 1983, and starting to get it s nose bloodied. In the coffeehouse that he frequented, Ahmed read everything about the war that he could get his hands on. With his heart fired by a righteous cause as only a young man s can be, he reached out for those who could get him to the battlefields in the Hindu Kush.

Joining others who traveled to Pakistan and then to the training camps, Ahmed began his training as a Mujihadeen. During those six years of combat operations, he was wounded twice and was rumored to have recuperated in Saudi Arabia.

In the 1990 s, Ahmed would become one of the core members of what would later be known as the "Abkhaz battalion". This unit gained a reputation of being a disciplined, well-armed, fierce fighting force capable of independent operations. Ahmed found alongside the Azerbaijanis in Nagorno-Karabakh and against the Georgians in Abkhazia.

By the time he was 30, Ahmed was a seasoned combat veteran who could speak and write North American English, Pushtu, Arabic and Russian. In addition to an array of Warsaw Pact and NATO small arms and light weapons, Ahmed was reasonably competent with explosives and basic electronics.

When the Russians invaded Chechnya in December, 1994, this unit was one of the key elements of General Dudayev s defense. Ahmed was also with Chechen field commander Basayev during the June 1995 raid on Budennovsk — some 90 miles inside of Russia.

Ahmed dropped out of sight from early 1997 to mid-1999, with some rumors placing him on the long fought-over "Line Of Control" in the Himalayan mountains.

When the Russians began to make hostile gestures towards Chechnya during the summer of 1999, Ahmed returned to that country. He was in the thick of the fighting until wounded in the fighting for Grozny in January, 2000. Evacuated through Georgia to a location in Lebanon to recuperate, Ahmed could only watch the satellite television news reports in fustration as Mujihadeen units were hunted down and eliminated by the Russians.

Meanwhile, Krasnovian agents had been scouring the old southern Soviet Republics for rumored caches of biological agents that were for sale to the right bidders.

When the message of success came in mid-June from the Krasnovian agents, those Jihad leaders who could be gathered weighed the risks and benefits. To a man, they decided it was time to carry the war back to the Great Satan.

*

Thus began the shell game to reach America. A series of planes, trains and automobiles brought him to a freighter crossing the Atlantic. During this time, Ahmed shaved his beard and let his hair grow into a length more sociably acceptable in western circles.

He also began the process of mentally thinking in English, after years of Arabic. Since he wanted to avoid contact with the mostly-Malaysian crew, he watched satellite TV beamed out of the United States and movie after movie on the cabin s VCR.

The bland, unsympathetic news reports and materialistic commercials only served to harden his resolve.

D—7
12 September 2005

The National Guardsmen were targeted long before the attack on Dartmouth ever began. Hasim had sat up late one night in May with the TV on, surfing the web until he found the Rapid Assessment Initial Detection (RAID) teams' website. On it, he found the names of the commander, a detachment Officer In Charge (OIC), and two senior sergeants. Taking these four names, he went to an online phonebook and searched through all the similar names in the state. While both officers had common names, there was only one entry for the senior-most sergeant's and two for other man. He noted this... and smiled. Sergeants do the real work in every unit

It only took a few minutes more exploration to find out that the unit was short four critical personnel (at least they were advertising for them). The links to their drill schedule and unit notes was disabled. Pity.

But what he had found that spring night was enough and had taken only 15 minutes to gather. He turned off the laptop and concentrated on the BBC World News...

*

Eric Foreman was driving home from his job to his home in Waltham. He yawned. Same stuff, different day. The only thing that bothered him was how to juggle his kid's soccer game this coming weekend with another National Guard weekend exercise.

Unlike most National Guardsmen, Eric was a full-time employee who usually had weekends off. So were the people in his unit. However, he was the First Sergeant — the senior Non-Commissioned Officer (NCO) of the 1st CIVIL SUPPORT TEAM (WMD)* — so he couldn t just ditch the weekend and make it up later. Maybe he could slid out for a long lunch on Saturday .

* Hereafter referred to as the 1st CST (MANG)

The back roads that Foreman used to avoid lights and traffic were lined with stone walls that had been there since the minutemen had chased the Redcoats back to Boston 225 years ago.

Foreman never noticed the 88 Dodge until it flashed it s highbeams and made to pass him. He shrugged, slowed down but the Dodge cut in sharply, catching his left rear with it s right front quarterpanel. This was actually a cop s trick to get drunk drivers off the road, but Foreman never knew that. He swung to the right and jammed on the breaks. That didn t stop the mini-van s slid off the asphalt and the right rear tire caught one of those ancient stones.

The minivan had rolled three times by the time the Dodge s headlights had disappeared.

THE WHOLE STORY

The 1st CST (MANG) was a 22-man Massachusetts National Guard unit formed in 1999. Since then, the members had trained to precisely identify nuclear radiation, as well as the presence of biological or chem ical weapons. In 2000, they still had not been given the Federal tests conducted at Fort Drum, NY that were designed to gauge how well they were able to respond to threats but by 2005, these units had been in existence long enough to become quite proficient at their jobs.

However, with critical names on the unit webpage and some of the key leadership without unlisted num bers, the Terrorists had only to see which one of their sympathizers was the closest to a man who kept a regular schedule.

Whether Foreman lives or dies is immaterial. Provided that the sergeant is competent, a military unit with out it s senior NCO can be more severely crippled than if it lost it s most senior officer. Foreman s acci dent would set the unit back at least three months, since his replacement would have to be found and brought up to speed

D—2
17 September 2005

GETTING INTO AMERICA

The freighter was just shy of the lights from Cornwall, Ontario on a cloudy night, when Ahmed was taken on the ship s Zodiac into the American side of St. Regis reservation.

There, in a house off by itself in the woods, Ahmed met an unkempt man who may or may not have been a Mohawk but was quite willing to provide him with the basic tools he d need for the mission. With an old .25 Beretta that he had brought with him within easy reach in his coat pocket, Ahmed laid an envelope of $100 bills on the table.

He took the keys to a blue 1990 Toyota Corrolla that had been purchased from an elderly woman no longer able to drive. Both men went outside and Ahmed started it up, let it idle and listened to the engine while he walked around it. It was acceptably anonymous and there were still six months left on the New York State inspection sticker.

The criminal had been led to believe that Ahmed was just another illegal immigrant, but some Ahmed s requests made the American doubt that story. Not that he cared, as long as the foreign guy had the money.

The second item that Ahmed was buying for an obscenely large amount of money was a .357 Taurus revolver that had been purchased from another poor widow. The weapon had belonged to her husband and was like the car, in that while technically improperly transferred, at least wasn t stolen. There was also a box of 50 cartridges to go with it.

The man also supplied him with a single blasting cap, a one-pound can of FFFG black powder, a 12" section of 2" diameter pipe threaded on both ends, and two matching end caps. With the sincerest sounding flattery, Ahmed had the criminal show him how to drill a hole in the side of the pipe.

*

The St. Regis Mohawk Reservation, located along the U.S. and Canadian border was considered the focal point of large scale alcohol and tobacco smuggling operations since the early 1990’s.

Where Canadian, American and Tribal law enforcement overlapped, there were seams that criminal elements quickly identified and exploited. In addition to narcotics and illegal weapons, the alcohol and tobacco was generally smuggled into Canada in an attempt to evade the payment of higher Canadian excise taxes. These schemes utilized warehouses on the St. Regis Mohawk Indian Reservation as staging areas.

Years later, a New York City-based ring was smuggling illegal Chinese workers into the United States through St. Regis. About 150 illegal immigrants a month were hidden in safe houses and then taken on the seven hour plus car-ride to New York City. An estimated 3,600 Chinese were brought in over two years, with each immigrant paying as much as $47,000 to travel the complicated route through two or three continents before ending up in Canada, where they were smuggled by boat across the St. Lawrence River.

After a year-long investigation, U.S. and Canadian law enforcement agencies arrested 35 suspects in December 1998. They estimated that 12 more escaped. The ringleaders faced federal conspiracy and alien-trafficking charges. As the U.S. attorney in Albany, N.Y., Thomas Maroney noted, "the geography of the (reservation area) is perfect for smuggling."

The St. Regis Tribal Police force assisted with the bust, but the force was only a few years old at that point. It had been formed after the last one was disbanded after the outbreak of violence eight years prior. In late 1989 and throughout 1990, the reservation was subjected to nightly volleys of gunfire and burning roadblocks as Mohawk was against Mohawk over the legalities of nine casinos along Route 37. A core-group of two dozen braves even faced down the Canadian Defense Forces on the northern bank of the St. Lawrence.

However, that police sweep didn t plug the hole in the two nation s border. There were always more criminals, Mohawks or not, who were willing to step into the vacuum and set up any sort of illegal operation you d care to name.

Ahmed was traveling under his old Canadian passport, which had been renewed a few years back. He even had a Canadian driver s license, which someone else had acquired. Amazing what a sob story, a recent photo and a bucket of money could accomplish with western civil servants.

As far as he knew, none of the western intelligence or law enforcement agencies knew his real name. Furthermore, the Russians had only sent INTERPOL Basayev and Khattab s photos — which told him that they didn t have any of the other fighter s information.

*

Ahmed had found the time, during the last 17 years, to read many books on military history and leaders, from Saladin to Schwarzkopf. One lesson that repeated itself quite often was that no plan survived first contact with the enemy.

This criminal who was supplying him with the car and pistol was content to drink whiskey and waste the rest of the night with small-talk. It didn t take long for Ahmed to deduce that the man was a potential security leak. It was not worth leaving him alive to bring another Mujihadeen into America this way. Ahmed was prepared to accept whatever repercussions might be associated with disposing of this unpleasant fellow.

Donning a pair of surgical gloves, Ahmed took the .25 and a soiled pillow from the couch. Placing both in one smooth motion against the criminal s head, the three tiny slugs were enough to make this look like another disagreement between smugglers.

That task finished, the traveler sat down and filled the pipe with powder. When it was properly closed up, with the blasting cap buried inside and only two lead wires protruding, Ahmed made the timer using two batteries, a small travel alarm clock and some tape. It was the crudest of time bombs, but it would serve his purpose.

Cleaning up the debris, he noticed that his schedule was working out nicely. He left, turning on the car s headlights only when he reached Rt 37. On the seat next to him was a stainless steel Starbucks thermos. By dawn, he was in Vermont.

*

D- Day
19 September 2005

THE TARGET

Hanover, New Hampshire is located in the Upper Connecticut River Valley, a region of small towns a few hours' drive from Boston and Montreal. The area was home to 95,000 residents, two-thirds of which lived in Hanover or Lebanon, NH, and Hartford or Norwich VT.

Hanover, considered to be the cultural anchor of the Upper Valley, has a population of well over 9,000 and is the home of Dartmouth College. Ahmed s target was Darmouth the United State s ninth oldest college and a member of the Ivy League. The private, four-year, liberal arts, coeducational college with schools of business, engineering and medicine as well as 16 graduate programs in the arts and sciences sat on a 200-acre main campus and had a total over 5300 students.

Student orientation always tried to offer an orderly beginning to each new year, but often devolved into chaos. The target were the first year students — the youngest ones, the Class of 2008. The Krasnovians decided that this target choice would hurt the Americans the most, if one could split hairs about such things.

Ahmed remembered the chaos of orientation and moving in day at the University of Toronto it was 18 years ago, but might have well been several lifetimes. No one noticed the dark-eyed, dark-haired man in the tweed jacket and jeans — just one more assistant professor in a sea of fresh faces.

It was quite easy to follow the gaggle of new students into the Alumni Gymnasium, since no one bothered with the security turnstiles during orientation. Ahmed eyeballed the auditorium as he approached, made sure no one was paying attention and pulled the can of shaving cream from his backpack.

He twisted the lid one-quarter of a turn and squatted, leaving it next to a trashcan at the back of the auditorium. This activated a five minute delayed timer, that would silently "mist" the room with the viral agent.

Ahmed, a firm believer in the "Keep It Simple, Stupid" principle, turned and strolled away. There d be plenty more opportunities to get imaginative with the delivery methods. This time, he just wanted to see if it really worked.

There was one more chore to be done. Carrying his "lunch" in a brown paper bag, Ahmed passed a US post office box. Juggling his shoulder bag and lunch like any harried Teaching Assistant, he got the mailbox door open.

No one noticed him dump a small cardboard box from the paper bag, right on top of the rest of the postcards waiting to be picked up that weekend. Inside that box was the crude time-bomb, set to go off in about 22 hours. With any luck, he d draw a few police investigators into the path of the virus.

"Amhed" returned to his car and pulled into traffic, enjoying the morning sunshine. He didn t mind the congested streets and lanes, filled with parents sweating under the loads of their little darlings belongings. The irony of their materialism being the catalyst to their divine punishment wasn t lost to his sense of humor.

This thought fueled his smile and he waved another couple across the street in front of him. Traffic was creeping along quite satisfactorily, thanks to the Dartmouth policeman moving things along at the intersection.

He was used to mindless waiting at the edge of horror and could do it now without raising his heartbeat a single pulse. The license plates of the cars around him were mostly from New York and Massachusetts.

He — and the student s parents - were two hours northwest of Boston and five hours north of New York City. This was good. Very good.

Ahmed headed out to Interstate 89.

*

Five minutes after he d finished chatting up the new coeds, Jeremy Pickering went back to toss out his empty coke can in the recycling bin. Something felt weird.. near the trashcan.

He shrugged to himself. Leading freshmen around was a total drain. Pickering slung the bag over his shoulder and dragged his sorry butt back to his room for a well-deserved map.

Of the 50 students that were dosed with the virus, five went to Boston that night to check out the all-night clubs. Five more were over to visit friends at Colby-Sawyer, a women’s college in New London, NH.

Forty stayed on campus, more or less preparing for the new school year.

*

D + 1

20 September 2005 (Tuesday)

INFORMATION WARFARE

After making a leisurely drive down to New York City, Ahmed had found Hasim in Manhattan with little problem. Having been to America a few times when he was in High School and also committing a mental image of the map of the SoHo to memory helped quite a bit.

The two men worked their way slowly through dinner at a vegetarian restaurant and it was after dark by the time they went back to Hasim s apartment. Ahmed got along quite well with the younger man, a brother in the great struggle who was born in Jordan in 1974. While the younger man had never carried a weapon in the struggle, he was quite dangerous in his own right as a well-trained computer programmer and occasional hacker.

Over the preceding year, Hasim had helped build several websites used by the Mujihadeens news organizations. When he expressed a willingness and ability to be more proactive in the cause, Hasim was allowed to demonstrate his skills to several fighters living in America. They were impressed enough to team him with Ahmed.

Three months prior, Hasim had engineered a virus into a pornographic internet movie (AVI) file and released it onto the internet. In a few days, over 1,000 fools with high-speed DSL* connections to the internet across America had downloaded his pornographic filth. When the time came, he would simply be able to send a command that turned their home personal computers into zombies .

***Alternatively, Cable Modem, T1or ISDN users could also be targeted.**

Hasim and Ahmed created a list of targets while they finished a pot of tea. Back at his apartment, Hasim used a laptop plugged into a stolen cell phone to launch a Denial Of Service (DOS) attack on Internet Service Portals serving central New Hampshire. This effectively shut down internet service in the targeted area by dawn.

> A Denial of Service (DoS) attack is not a virus but a method hackers use to prevent or deny legitimate users access to a computer. DoS attacks are typically executed using DoS tools that send many request packets to a targeted Internet server (usually Web, FTP or Mail server), which floods the server's resources, making the system unusable. Any system connected to the Internet equipped with TCP-based network services are subject to attack. For example, imagine a hacker creates a program that calls a local pizza store. The pizza store answers the telephone, but learns that it is a prank call. If the program repeats this task continuously, it prevents legitimate customers from ordering pizza because the telephone line is busy. This is a denial of service, and analogous to a DoS attack. - from SYMANTEC s webpage (http://www.symantec.com/avcenter/venc/data/dos.attack.html)

D + 2
21 September 2005 (Wednesday)

In Manhatten, Ahmed and Hasim scoured internet news sites until they found a brief mention of the Dartmouth pipebomb in a small paper s online site. For Hasim, it was somewhat unsatisfying to see that it only received the attention of one of the local detectives, and not the New Hampshire State Police. Ahmed reassured him that, when the time came, that tiny toy would be worth it s weight in gold for the confusion it helped cause.

There was nothing to be found about the random closures of ISPs in New Hampshire, but Hasim figured that it would take another day for that to become news — if it happened at all. The attacks had only lasted an hour, this time, since the mujihadeen wanted to see how the Americans would react.

*

D + 3
22 September 2005 (Thursday)

OUTBREAK

Jeremy Pickering wondered how anyone can get a cold in the middle of September. It was horrible being sick on the first day of classes. It was even more horrible when the people next to you were sick too, and you were a million miles away from home. He d been up at Dartmouth for three years and hadn t been sick once. On top of that, both his roommate and his girlfriend had probably picked up whatever he had and were both ticked off at him.

It was the worst cold he d ever had, but Jeremy had bagged going to see anyone about it Sunday. He knew he d have to wait forever to see a nurse or doctor, so he just gobbled down some Motrin and slept most of the day.

By Thursday morning, he was completely wasted. His buddies had helped him and his roommate to get down to the school infirmary. This was going to completely mess up his sched-u l e

The Nature Of The Agent

The Hanover Virus was a powder, stable in dried form, and roughly equivalent to Anthrax in the amount of agent needed to infect a given area. It incubates over a three to five day period before first symptoms the first symptoms appear — usually as a cold or upper respiratory infection and go on to become encephalitis. High fevers, head-aches, nausea and vomiting, seizures and ultimately a "cooked brain" will be the result unless victims receive support.

There is no treatment and without care, roughly one-third of those infected will die. It takes about three days to one week to succumb, depending on the strength of the host. Typically, the very young and the very old are the most vulnerable.

The bioengineered altered plague 1- 5 nanometers across filled with genome from several different altered agents, with two or three agents in each sphere. The spheres were also coated to disguise them from rou tine detection by present methods.

The Semantics Of Disease
Plague and Virus are often used interchangeably by the layman. Strictly speaking, the two are quite dif ferent and the indiscriminate use of one term for the other can lead to confusion amongst both medical professionals and laymen.

A) Definition Of A Virus

Viruses are organized associations of macromolecules:- nucleic acid (which carries the blueprint for the replication of progeny virions) contained within a protective shell of protein units .

On its own, a virus may be considered as an inert biochemical complex since it cannot replicate outside of a living cell. Once it has invaded a cell it is able to direct the host cell machinery to synthesize new intact infectious virus particles (virions).
Because viruses are non-motile, they are entirely dependent on external physical factors for chance move ment and spread to infect other susceptible cells.

B) Clinical description of Plague
A disease characterized by fever and leukocytosis that presents in one or more of the following principal clinical forms:
- Regional lymphadenitis (bubonic plague)
- Septicemia without an evident bubo (septicemic plague)
- Plague pneumonia, resulting from hematogenous spread in bubonic or septicemic cases (secondary plague pneumonia) or inhalation of infectious droplets (primary plague pneumonia)
- Pharyngitis and cervical lymphadenitis resulting from exposure to larger infectious droplets or ingestion of infected tissues (pharyngeal plague)

Plague is transmitted to humans by fleas or by direct exposure to infected tissues or respiratory droplets.

Laboratory criteria for diagnosis
- Isolation of Yersinia pestis from a clinical specimen, or
- Fourfold or greater change in serum antibody to Y. pestis

At least 75 cases of upper respiratory infection and seizures had flooded Dartmouth s infirmary by the end of the day and that night, the most severe cases were transferred to the closest area hospitals.

The Upper Valley had two medical facilities: the newly-built, multi-faceted Dartmouth-Hitchcock Medical Center (a modern 400-bed tertiary care hospital, research and clinical facilities for Dartmouth Medical School. Referred to as DHMC) and Alice Peck Day Memorial Hospital (Alice Peck Day Memorial Hospital is an up-to-date community hospital, with 82 beds and 250 employees - over 60 of them physicians and allied health professionals, in 22 specialties and clinical areas.). The DHMC was in nearby Lebanon, the largest community within the Upper Valley (population 12,231.

D + 5
24 September 2005 (Saturday)

The first deaths occurred on Saturday — two fever cases in the DHMC shot up to 106 degrees. Within 12 hours, there were eight more deaths in the immediate Dartmouth area, although five of them were outside of the school s population.

D + 6
25 September 2005 (Sunday)

It wasn t until Sunday morning that DHMC s staff realized that they had a serious outbreak on their hands. An estimated 200 students had fallen ill. The area s hospitals and medical centers were alerted to a probable flu outbreak.

In the Merrimack Valley region, there was the Southern New Hampshire Medical Center (Nashua), Catholic Medical Center (Manchester - 333 beds), Concord Hospital (Concord - 295 beds), Parkland Medical Center (Derry - 86 beds), St. Joseph Hospital & Trauma Center (Nashua - 218 bed)

There was also the Salem Family Practice and Walk-In Center (Salem), the Cypress Center/Mental Health Center of Greater Manchester (Manchester), and the Charter Brookside Behavior Health System of New England (Nashua - 100 beds).

In the Monadnock Region, there was the Cheshire Medical Center (Keene - 177-bed acute-care hospital serves as a regional medical referral center), the Monadnock Community Hospital (Peterborough - 62 beds).

Considering the number of beds already occupied on the 24th, this didn t leave much capacity if more people fell ill.

Near the immediate area, there was the Veteran s Administration hospital in White River Junction. There was also a significant telemedicine system in place in Northern Vermont and New York, that connected 12 hospitals with real time interactive video.

*

D + 8
27 September 2005 (Tuesday)

The Hanover Police Department had 19 full-time officers and 11 full-time civilians (including dispatchers, parking and administrative employees). The Chief called in all his favors and managed to get most of his patrolmen to work extra shifts. He also brought in three reserve officers (who usually handled church traffic on Sundays) and four men who had retired in the last five years.

It wasn t enough. Things really went to hell during the course of the day. At first, it was traffic problems around the CVS and other pharmacies, some fights in checkout lines that needed to be broken up. Someone mentioned that their church service that morning sounded like a TB ward.

Rumors spread from the campus throughout the town, particularly when the parking lots at the area emergency wards started to overflow onto surrounding streets. By 1 PM (13.00), DHMC had registered 300 fever cases of unknown origin and called the Center for Disease Control (CDC).

Some of the more vocal "townies" blamed what was happening on the influx of rich kids" at Dartmouth, and the Hanover police had to waste the time of four officers responding to a series of beatings. By afternoon, a patrolman reported that one frathouse appeared to be undergoing a massed exodus.

*

The wheels of government turned slowly at first, with about a dozen New Hampshire State Police cars and a mobile command center bus showing up to help Hanover s chief. The New Hampshire Office of Emergency Management (NHOEM) was activated as well.

> The NHOEM is a state agency charged with the preparation for the carrying out of all emergency func tions, to prevent loss of life or property resulting from any natural or man-made cause, but not limited to fire, flood, earthquake, windstorm, wave action, oil spill, or other water contamination requiring emer gency action to avert danger or damage, epidemic, air contamination, blight, drought, infestation, explo sion or riot.

The NHOEM had been pursuing a noble effort to prepare for situations like this, with training like the COBRA (chemical, ordnance, biological, and radiological), WMD Responder Training Course COBRA, WMD Incident Command Training Course COBRA, WMD Hazardous Material Technician Training Course, Comprehensive Emergency Management Planning for Schools (CEMPS) and Emergency Response to a Criminal/Terrorist Incident classes. However, no one knew that they were facing an engineered biological attack at that point.

MISDIAGNOSIS & WRONG ASSUMPTIONS

The medical community had to jump through hoops that Tuesday as well. The last time anything like this had happened naturally was an outbreak of enterotoxigenic Escherichia coli (ETEC) back in 1993. The number of critical cases quickly overtaxed the local fire department EMTs and ambulance companies; CarePlus (Lebanon), Golden Cross Ambulance, Inc. (Claremont) and Upper Valley Ambulance, Inc (Fairlee, VT).

With the symptoms in the first patients, the people in the OEM thought they were dealing with just another flu at first. "Fall Flu Outbreak" was the title written on most of the planning boards and with the fears of another pandemic growing every year, researchers were looking in the wrong direction.

Luckily, the OEM was able to have several ambulance companies dispatch vehicles to the DHMC but it was like trying to stop a flood with a spoon. As it grew later on a Sunday afternoon, it would become harder to gather assets to deal with massively expanding number of sick people in the Hanover and Lebanon area.

They also convinced the governor to alert the New Hampshire Army National Guard. Their initial request was for transport, tents, medical personnel and some soldiers for crowd control. Since most of the units weren t on drill status that weekend, it would take them hours to assemble and even more time to get to the site.

The first New Hampshire Army National Guard unit to respond to the Governor s call was "C" Company, 3-172d Infantry Battalion (Mountain), whose armory was in Lebanon. The unit had been on their normal weekend drill when they were given orders at 3 pm (15.00) to assist the New Hampshire State Police in maintaining control of Hanover.

Subtracting those who had gone home already, less than 100 Guardsmen were available. While trained to fight on foot in mountains, they only issued crowd control gear — clear plastic facemasks for their kevlar helmets, body armor, wooden riot batons and their M17 protective masks (with hoods).

Not a single member of the company was armed, since National Guard protocols required the separate storage of ammunition. Besides, this was described as more a matter of traffic and crowd control than anything resembling a military operation.

They though their most difficult task would be setting up their tents on the DHMC s lawn.

Overhead, a Blackhawk from the 1159th Medical Company (Air Ambulance) in Concord buzzed past. The second New Hampshire National Guard unit to receive the alert was already ferrying the worst cases considered moveable to hospitals in northern Massachusetts.

> The mission of the 1159th Medical Company is two-fold. In wartime, the mission is to help conserve the fighting force by providing aeromedical evacuation support and services within the theater of operations. In peacetime, the mission is to provide aviation assets to protect life and property and to preserve the internal security of the state when ordered by the governor. The unit transitioned to UH-60 Blackhawks in 1998. For purposes of this scenario, the 1159th has four flying Blackhawks.
> http://www.nhguard.org/1159med.htm

*

Ten minutes after C Company s trucks pulled out of their armory parking lot, Leroy McCoy was on the phone. With all the weirdness going on around the hospitals and that secret government lab at Hitchcock Medical, it didn t take a Ph.D. to see what was happening — not with the Guard hustling out of their armory on a Sunday afternoon and black helicopters shuttling up towards Hanover.

He spoke only three words, then hung up. Grabbing his car keys and lunchbox, Leroy left work at the Pep Boys without saying a word to anyone. Leroy was a member of a Constitution Defense Militia squad and this clearly was an event .

*

CONTAINMENT

Based on the New Hampshire State Police reports, officers from C , D and F troops set up the first roadblocks in a rough perimeter around the Hanover area about two miles outside of town on Routes 10 and 120.

In planning to deal with whatever this emerging but still unidentified problem, the NHOEC and the Vermont Emergency Management established a series of forward command posts about 25 miles from the Hanover/White Junction/Hartford/Lebanon area; to the south, Springfield; to the east, George s Mill; to the North, Piermont/Piermont Station; and to the West, Bethel. Using Routes 91 and 89, the Combined Operations Center planned to set up only four major roadblocks to funnel refugees into holding areas.

It took most of the morning for the other Guardsmen from New Hampshire s 2nd Battalion/172nd Field Artillery and 2nd Battalion/197th Field Artillery battalions to gather at their armories, draw equipment and begin civil disturbance refresher training.

The bulk of the 2d Battalion 197th Field Artillery (Headquarters, Headquarters & Service and A Battery) were in Berlin and able to gather 200 men. Units from the 2nd Battalion/172nd Field Artillery in Nashua and Milford joined them.

In Hillsboro, the 744th Transportation Company and a detachment in Claremont were able to reach the area around 2 PM. These 18-wheeler cargo carriers first mission was to haul stretcher cases south to Springfield VT, where temporary accommodations had been set up in the schools.

> The mission of the 744th Transportation Company is to provide transportation for the movement of both dry and refrigerated containerized cargo, general non-containerized cargo, bulk water, and bulk petroleum products by motor transport. The unit s M915/A1 18 wheeler semi-rigs with 400 horsepower diesel engines capable of hauling a 50 ton load.
> See http://www.nhguard.org/det1744.htm or http://www.nhguard.org/744trans.htm

With the situation worsening by the hour, Vermont activated their Division of Emergency Management at Waterbury at 08.00. Since the Hanover Virus was already straddling the Vermont/New Hampshire border, the Vermont National Guard was activated one hour after their neighbors. The 1st/172nd Armor (from St. Albans) and 2nd/172nd Armor (from Rutland) Battalions were tasked with maintaining roadblocks around the Hot Zone.

The Vermont National Guard s 186th Forward Support Battalion (FSB) in Northfield set up operations in Barre. FSBs have been likened to a grocery store, service station, parts supply store and truck dealer all in one and are quite useful in providing refugee assistance.

CHAOS THEORY & SCARED, ANGRY PEOPLE WITH GUNS

Around 18.00, the small 1st CST convoy crossed the New Hampshire/Massachusetts border. As they passed Manchester and Concord, traffic heading the other direction started to thicken, which told the Massachusetts Guardsmen that this cold alert was anything but another drill.

The section was doing it s best since the loss of First Sergeant Foreman, but they had still taken too long to get out of their armory. There was an accident that closed Rt 89 near Lake Sunapee, so Captain Flores had the convoy make a quick detour up to 4A.

They passed Springfield around 20.00 and not five minutes later ran into what could only be described as a roadblock. Two sergeants went to investigate the old hay wagon that was blocking the road while Flores was on a cell phone to the NHOEM.

He heard some conversation that was turning louder out in the darkness and had just ended his phone call when two shots rang out, followed by yelling. The sergeants came back, one supporting the other and both swearing.

Someone in a mask had come out from the side of the road, asked who they were — where they were going — what authority they had for trespassing in New Hampshire. Both Guardsmen had short tempers and were somewhat curt with their answers.

From beyond their range of nighttime vision, someone had shot at them twice. One bullet had found it s mark, but not fatally.

Flores was enraged but helpless. They weren t armed and their mission didn t involve gunbattles with idiots. He had the convoy turned around in three minutes and headed towards West Springfield, then Grantham and Rt 89.

> In 1966 racial discrimination, economic injustice and the Vietnam War sparked 21 major riots and civil disturbances. In 1967 there 83 such incidents. A third of the 83 were marked by incidents of sniping. In more than half of them, looting took place. The National Guard was required to suppress 25.

D + 9
28 September 2005 (Wednesday)

Homeland Defense in Action

When it became obvious that the Hanover problem was more than just a larger than normal flu outbreak, researchers started looking at different strains. During the 20th century, pandemics had occurred about once every 30 years.

In 1918, it was the Spanish Flu — considered the most deadly pandemic in recent history, killing more than 20 million people worldwide. In 1957 and 1968, pandemics affected mainly the elderly and chronically ill. In 1976, it was Swine Flu and in 1997, Avian Flu, but neither really "counted" as a pandemic. So the infectious disease community had figured that America was eight years overdue for a new Flu.

In those eight years, the American medical community had made great strides in dealing with naturally occurring diseases (to include an overhaul of the drug manufacturers in 2002-2004). Another step in the right direction happened in the first years of the 21st century, America had taken some small but proactive steps against Chemical and Biological Homeland attacks. In addition to the National Guard teams, the internet was used to link medical planners and facilities across the country.

Unfortunately, it was impossible to effectively fight the unknown and the well-meaning professionals wound up boxing shadows. Since no one was familiar with this engineered virus, every initial diagnosis was wrong.

The CDC claimed it was a Pox Virus, and recommended a treatment regime.

The First Responders in New Hampshire handed out simple face masks.

The Spanish Flu of 1918 — The Model For Horror

The first reported case of the Spanish Flu was on 11 March 1918 when Private Albert Githell, 89th Infantry Division, reported sick with a sore throat, fever, and headache at Fort Riley, Kansas. By the end of the week, 500 soldiers had fallen victim to the flu. Within a week it had swept across America; In a short time, the flu made it's way to 46 states and it took only three months to take the world by storm.

Not only was the Spanish Flu strikingly virulent, but it displayed an unusual preference in its choice of victims---tending to select young healthy adults over those with weak ened immune systems, as in the very young, the very old, and the infirm. During this first but least powerful of three waves, the flu began to die out shortly after it had spread.

By fall, America was hit by the second and most powerful wave, with the number of dead in thousands. The bulk of the flu passed by late December, leaving an estimated 675,000 Americans dead and 20 million seriously ill citizens fighting the disease. Nearly 200,000 deaths were recorded in just the month of October 1918. On 1 July 1917, the population of the United States was 103,268,000. By 1999, it was 272,690,813, so an equivalent loss at the end of the 20th century would have been 4,715,000 dead and 54 million sick.

The third wave, in early 1919, may have been only a fluctuation of the second wave. Worldwide, the mortality figure for the full pandemic is believed to stand somewhere between 30 to 40 million. An estimated 0.5% of the UK population died, along with 5% of communities in Africa and India, whereas in some isolated groups (particularly Alaska, central Australia and Samoa), the mortality rate was 60%.

"As their lungs filled the patients became short of breath and increasingly cyanotic. After gasping for several hours they became delirious and incontinent, and many died struggling to clear their airways of a blood-tinged froth that sometimes gushed from their nose and mouth. It was a dreadful business".
--Isaac Starr, 3rd year medical student, University of Pennsylvania, 1918.

D + 10
29 September 2005 (Thursday)

By 10 a.m., life was not good at the NHOEC. Reports from the field were growing worse by the hour. Many of the first responders were now patients. Sterile zones were broken in the emergency aid stations, time and again.

Within the 25 mile perimeter, life can to a screeching halt. Business shut down and most folks "hunkered down" just like they would for a bad snowstorm. A small minority of the population — estimated to be about 10% - panicked and tried to leave for anywhere else. Most of them were stopped at the perimeter checkpoints.

The 911 system in central New Hampshire shut down and a few accidents on I-91 turned a five-mile section of that road into a parking lot.

Outside of the 25 mile perimeter, the media descended like the Biblical plague of locusts and some of them even slipped into past the cordon. All of them — print, television and internet — put a tremendous strain on the local telephone net. New Hampshire was fairly remote for the East Coast of the United States and hadn t had digital service for very long.

Worse was that for the last hour, no one could get an outside computer line — in addition to the regular portals, all of the commercial lines were down or permanently busy as well. The information freeze was maddening, since the voice lines were already overwhelmed.

The most distressing incident was when WEVH 91.3 fm (Hanover/Upper Valley) went off the air at 11.00. Most OEM observers attributed this to a brownout, but it was later determined to be due to a fire of undetermined origin that damaged the station generator.

At noon, the President of the United States appeared before the White House press corps and declared the Upper Connecticut Valley a disaster area and placed it under martial law. After consultations with seven governors, emergency procedures were enacted across New England;

most public events were cancelled and their state national guards activated. He appealed for national calm and prayer, and promised to keep the nation updated. His prepared text was over in two minutes.

*

At 1 p.m., the Crisis Commander shut down the cell relay banks and, save for a small pool of reporters, moved the herd of media vultures to an alternate command post 75 miles away. Within an hour, the communication situation had regain some of it s vitality, but it was too late.

The DHMC reported that they had 300 corpses stacked up like cordwood and an indeterminate number of patients about to join their recently-deceased neighbors.

When pressed for a projected "worst case" for the week ahead, the NHOEC staff replied "several thousand" before the Hanover Virus burnt itself out. Of course, no one really knew then. It wasn t even an educated guess.

From within the perimeter, more aid workers were showing signs of infection. The on-site OEC staff had decided to go it alone and requested that no one else be sent into the Hot Zone.

*

By nightfall, the President had ordered elements of the Armed Forces to the second perimeter — mostly medical and support units, people to purify water and ship supplies. While incidents of public disobedience and looting where thankfully few and far between, Military Police units were also being flown the New England area.

The President addressed the nation again, sharing his concerns that the crisis could broaden and effect national interests. He explained to a worried nation that he had held early morning meetings with the Joint Chiefs, the Security Council and the Senate, before enacting elements of the Emergency Powers Act.

D + 11
30 September 2005 (Friday)

And the virus spread further ....

In New York, the stock market started to react with predictable volatility and the press made it seem was movies like the "12 Monkeys" and "Outbreak) or books like "The Cobra Event", "The Hot Zone", and "Rainbow Six" come right to the public s doorstep.

Outside of Boston, the parents of Kevin Matthews were both in bed with the worst colds they d ever gotten. In New York City, Kitty Bierstein was chasing ALEVE tablets with Smirnoff and cursing the day she thought it d be a good idea to help her daughter move in at Dartmouth.

As dawn broke twenty miles south of Hanover, Joel Breckinridge was making good time on Appalachian Trail. The trail is a continuous marked footpath that goes from Katahdin in Maine to Springer Mountain in Georgia, a distance of about 2160 miles. He had been on it for a week already and it was going to be the best fall he d ever seen.

*

That morning, at 8 o clock, the President of the United States returned to the airwaves. He told the nation that the "terrible national crisis" had been contained in the New England area, but that those in the Hot Zone would have patience until the Hanover Virus burned itself out.

There were the inevitable barrage of questions from the Press Corps, but the only one addressed by the President was the likelihood that this was an act of terrorism. With a straight face, he told America that no one had taken claim for it and with the actual nature of the Hanover Virus still a mystery, no one was jumping to conclusions.

With that, the briefing was over

*

In Concord, the world began to fall apart at least in the New Hampshire OEM. Within two days, the first perimeter — 25 miles from Hanover - collapsed when National Guardsmen and State Police officers on the checkpoints began to show signs of infection.

The second perimeter had been set up about 50 miles out from Hanover. Beyond that perimeter, another huge problem smoldered — with the sudden blanket of media attention, the "walking worried" started to clog emergency rooms from Boston to Syracuse.

Terrified by what they saw, or didn t see, on TV, these completely healthy individuals drained the health system of time and energy that would have better benefited those who were actually sick.

The media seized the Hanover crisis with it s usual fervor and released a torrent of reports — most were useless to people inside the "Hot Zone". However, the commercial media reproduced the Government instructions often enough that when the CDC s website crashed from an incredible amount of traffic, there were plenty of alternate outlets available to take up the slack.

In New York City, Ahmed turned off the TV. He admired the way the American president had handled the situation. In due course, he d give His Excellency the American President something a bit more concrete to talk about.

*

Other cities hit with the "Dandelion Effect" weren t so lucky. Hospitals in downtown Baltimore reported 2,then 7, then 17 cases within hours of each other. With so many families with less-than-attentive HMOs, and an almost equal number without family doctors, it was easier for the Hanover Virus to slip through the cracks.

The city that was, as one sardonic official put it, "five minutes from a riot on a good day" got ugly. The Maryland National Guard was activated by the governor and tasked with protecting hospitals and their employees. BWI was closed to all flights, while I-95 and I-895 were closed north and south of the city.

*

While the President had been correct, in telling America that the Hanover Virus had been isolated in New England, the cases that cropped up across the world did hurt his credibility. Outbreaks, thankfully much smaller than in the Upper Connecticut Valley, in Boston, Baltimore, Pittsburgh and two of New York City s boroughs continued to tax the American medical health system to well into 2006.

Inside the perimeter, it took four months for the Hanover Virus to burn itself out. By the time the quarantine was lifted, over 5,100 Americans had died from this engineered virus.

An Alternate Reality, Or What Could Be Done

What would it take to stop an outbreak like this?

Even with only a few short years, there is enough existing technology to lay the foundations for a medical defense system that could not only be used to counter biological attacks, but also treat naturally-occurring medical emergencies across the globe.

The problem in both a biological warfare situation or naturally-occurring medical emergency is to detect the problem rapidly, while isolating and stabilizing those infected until a cure can be produced.

This means that doctors and medical specialists must have access to the problem to create a solution, and that supplies and humanitarian aide be provided — all without exposing those who are trying to solve the crisis.

Such a system must also be globally deployable. With a world that is increasingly interdependent and with air travel able to carry germs across the planet within a day, outbreaks can threaten the entire population. The best way to deal with problems like these are at the source, but the chances are that the epicenters will be in Earth s most remote corners.

The creation of a Medical Command & Control Telemedicine Net (MCCTN) is one solution — using laptop computers and the internet to link doctors, medical experts and databases across America (and possibly the world), literally the expertise of thousands of professionals could be focused anywhere in the world a bank of satellite or cell receivers could be set up.

The second "leg" of the MCCTN is the part that interfaces with those inside the "Hot Zone". Using robots originally developed by the military for battlefield surveillance and mobility, some of these same vehicles could be directed to carry humanitarian supplies, conduct medical reconnaissance and communicate with those who are infected.

The third "leg" of the MCCTN is education and awareness. With the potentially high percentage of uninfected walking worried capable of overtaxing a medical system that is already fighting a real problem, the general public needs access to information in such a way that panic is averted.

The MCCTN is also a coordinating agency, much like NASA marshaled America s resources in the 1960 s for the Apollo missions. However, this project went far beyond the medical community.

When the project was started, those involved realized the substantial costs that would have to be borne while putting the foundations in place. Where ever possible, the MCCTN would use existing systems and materials in the commercial, medical, military and scientific fields. Whenever possible, the MCCTN would be used for other missions beneficial to the country.

D + 4
The Other 23 September 2005 — MCCTN In Action

When this situation was declared a medical emergency, doctors in New Hampshire were linked to Maryland, New Mexico, the U.S. Army Medical Research Institute of Infectious Disease at Fort Detrick and the CDC under MCCTN. The system was activated with a simple email to the group s 11,000 volunteers.

The system wasn t anywhere near completion but considering that it had been created from scratch only three years before and that the members had had only one full-scale drill, the system worked.

Not perfectly, but it worked.

The initial benefit of the MCCTN was that it allowed New Hampshire s First Responders — volunteers with the most rudimentary of medical training — to interact in real time directly with physicians, immunologists and other experts on portable wireless laptops.

The plan was to get one Doctor online for every twenty patients and one nurse for every three patients, rotated every eight hours. The system mustered 200 physicians, 500 nurses and a slew of mental health professionals, all of them volunteers.

For the medical layman, this was the equivalent of the Pentagon talking directly to Army scouts half a world away or NASA s mission control seeing everything an astronaut could broadcast home from his helmet camera.

*

While information was flowing out of the Hot Zone, help was flying in. That night, a flight of CH-53 helicopters brought a detachment of specialists and heavy boxes on pallets from the Army s Test and Evaluation Command (ATEC) at Aberdeen, Maryland to Hillsboro.

The mechanics of the 744th Transportation Company started bolting robotic "drivers" into the cabs of their HEMMETs. Originally created to allow resupply on a chemically-contaminated battlefield, these black boxes, mechanical links and optical/thermal sensors created smart trucks that would now be carrying food and medical supplies to Hanover. The dozen trucks were controlled by through a bank of simulators in Fort A.P. Hill, Virginia, their drivers the instructors who taught "smart truck" courses to new soldiers.

The same was true for a dozen Unmanned Air Vehicles (UAVs), pilot-less helicopters ranging from tiny to normal-sized, that came from Fort Rucker, Alabama. The "pilots" for these were sitting in the U.S. Army Research Institute s Rotary Wing Aviation Research Unit, and those assigned to reconnaissance had military doctors with MCCTN laptops sitting right next to them.

Fifty miles away, at the other end of the Cordon around Dartmouth, two more helicopters were dropping the last of their enhanced motion sensors in the New Hampshire woods. Like a store s security camera, the thermal images from this ring of sensors were monitored at a MCCTN control station.

If necessary, infectious disease respiratory isolation-equipped teams of NH State Police would be dispatched to intercept anyone breaking the perimeter.

By midnight, a containment perimeter had been completed around Hanover and the NHOEC workers began to relax a bit.

D + 5
The Other 24 September 2005

The swarm of media descended on Concord, New Hampshire at 7 that morning, while towns just outside of the containment perimeter in Vermont began reporting them an hour later. Predictably, cell and ground wire communications capabilities began to be taxed to their limits.

The MCCTN and FEMA tried to compensate for the communications problems by broadcasting instructions on satellite and cable TV. While most of these could be characterized by the simplistic "No Human To Human Contact Except Through Barrier Suits", there where intangible moral builders — footage of volunteers across America packing food, water and humanitarian supplies onto Air Force planes. These were followed by aerial shots of the pallets being para-dropped onto Dartmouth s center square.

For an elderly widow in Hartford, it was a comfort that few could appreciate.

*

Outside of the DHMC, the Army s heavy UAVs had delivered a bank of Autonomous Medical Diagnosis Stations (AMDS). Not much bigger than a porta-john, these self-contained stalls had only to be plugged into a power source and their modems initiated, and DHMC had a dozen more doctors diagnosing patients already triaged by the First Responders.

What these AMDS lacked in the comfort of a human touch was more than made up for in the peace of mind of both those infected and those who would treat them.

While the rest of the world watched First Responders in Containment Suits waddling around with boxes of supplies, the same-pilot-less heavy helicopters were taking out patients in Containment Stretchers — hermetically sealed boxes with integral oxygen supplies. When they reached the airfield at Concord, the CS boxes were shuttled to hospitals within a 200 mile radius that were prepared to deal with isolation cases.

By mid-afternoon, only ten Hanover residents had died of the Hanover Virus.

*

No system is 100% perfect but thanks to the MCCTN, medical professionals across New England had been alerted to the probability of the "Dandelion Effect". Like the flowering weed;s seeds are carried on the wind, infected patients will infect more and more people as they travel.

When the Mathews called their family health care provider and described the symptoms, the nurse was tempted to just write them off as another pair of the "walking worried". Harold s hacking cough made her think twice about that unseen diagnosis and she stayed on the phone long enough to read their family file.

One son, Kevin, enrolled at Dartmouth College The nurse had a specially equipped EMT ambulance dispatched to the Mathews house within ten minutes.

There were a handful of other cases that were caught in the days that followed. Additional National/Federal Command Teams had to be sent to Boston and Baltimore, as well as CDC Reaction Teams with some basic supplies and portable labs.

But the catastrophe that could have been was averted.

2025
Combined Bio and Cyberthreats

Team 4

- Creating a War where the U.S. "attacks itself"
- Our approach results in a covert takeover without involvement against the U.S. military
- Taking advantage of the inherent weakness/fragility/culture of the U.S. social system
- Response to the attack creates infringement upon U.S. freedoms which alienate people from government (and eventually the military)
- Offer "a way out" (which is advantageous to us), leaving us in "control" of the U.S.

Key Concepts

- The "best" attack is one you (US) does not detect
    - Complex systems and "natural stupidity" are difficult to distinguish from "terrorism"
    - Keep US military out of the "problem"
    - Put no one in charge (US)
        - * Confusion between local/state/national governments and agencies as to "whose problem this is"
- Disabling/non-lethal better than destructive/lethal
- Use existing institutions/companies/trade associations to implement means
    - Buried/hidden in code and embedded systems
- Inexpensive to do and potentially profitable
    - Requires very few people (Red only "lights the match")
    - Technology exists; driven by commercial sector
        - * Red technology will develop faster (much) than Blue
        - * Low entry costs

Day 1

- 220001SEP25Z
- Major earthquake in southern California
    - President declares "national disaster area"
    - Fires break out in LA inner city
    - CNN announces may be related to underground test at Yuma

Day 1 (Continued)

- Rash of trucking related traffic accidents, during rush hour, at major cities CONUS wide
  - Partially disrupts flow of relief supplies
- Implementation of new approach to health care using telemedicine and robots
  - 1,000 Island Approach in LA;
    - * LA is broken down into districts, assigned to a responder city for telemedicine hookups over internet
    - * Service robots sent in for evacuation, support, clean up

Day 2

- Media reports poor/uncoordinated FEMA response to earthquake
  - Food/water/medical shortages
  - Transportation systems unworkable
  - "Wrong" relief supplies delivered to disaster area

Day 3-7

- Civil unrest in LA and throughout southern California
  - Governor activates state ARNG
    - * Declares martial law
- President declares situation "under control"
- Media reports situation "out of control"
- President denies he made declaration regarding status of situation in California
- Due to civil unrest, mass exodus from LA/southern California area
  - Traffic accidents/delays abound
  - Media reports severe accident involving Getty family members
  - LA effectively out of life support resources

Day 8

- Hanover, NH
  - Dartmouth College
- Half dozen students noted ill from unknown disease; thought to be outbreak of flu
- Hospital infectious disease investigating unusual outbreak of flu
- LA
  - Speaker of House calls for censure of President and cabinet for poor management
  - Footage of National Guard opening fire on inner city children attacking food distribution center in Watts

Day 8 (Continued)

- Hurricane hits Miami, FL
    - 17 foot tidal surge

Day 12

- Hanover, NH
    - Dartmouth College
- Hospital overloaded with sick students and medical personnel coming down with flu-like symptoms. Deaths have occurred.
    - son of prominent Senator Freeman dies
- Similar flu-like symptoms have appeared in New London, Boston, NY
- CDC announces this is not related to West Nile virus; CNN reports that there have been public health service announcements contrary to CDC s announcements
- CDC sends personnel to Dartmouth Hitchcock Medical Center
    - CNN shows CDC personnel in Level 4 containment suits
- LA
    - Civil war
    - Mayor of LA requests for military aid to replace ineffective ARNG; President denies request
- Miami
    - Requests to be declared national disaster area; President denies request
    - Miami protesters surround federal buildings

Day 15

- East Coast Epidemic Spreads
    - NY through DC and Atlanta now affected
        * Numerous prominent families affected
        * Hospitals overwhelmed
        * Government forced to evacuate, shutdown
    - CDC identifies infectious agent
    - CNN reports that Ft. Dietrich has variant
        * Ft. Dietrich denies
- President asks governors to declare quarantine
    - Closes commercial travel
    - Several governors refused
        * Federal troops deployed to enforce quarantine
        * New Hampshire agrees to quarantine but refuses federal troops
            - Fire fights between local militia and state troopers

Day 20

- East Coast Epidemic Spreads (third wave)
  - Chicago and St. Louis now affected
  - Continuing problems with distribution of relief supplies
  - Congress asks for President s resignation
  - All government functions are non-functional
    - * Bunkered
  - CNN reports it was a bioengineered agent; projected death rate of 5% of population weekly
    - * Unclear if slip or attack

Day 21

- President refuses to resign; promises new plan will work
  - Foreign countries offer aid
- President Announces 1,000 Islands response to epidemic
  - seal off all infected areas
  - Cities are paired for telemedicine (uninfected Phoenix is assigned to help hot-zone Chicago)
  - Prototype robots and automated transported key to radical plan for delivery and objective administration of resources and medical antidotes
- New Hampshire has declared it no longer sees value in remaining part of the Union
  - Federal troops enter NH to re-establish order
- CNN reports that senior leadership or families have over 20% fatalities from epidemic

Fourth Week

- Presidential plan fails
  - Telemedicine network is corrupted
  - CNN shows footage of 2 deaths due to "spoofed" telemedicine, footage of robots out of control
  - Isolated cities are not receiving any supplies
  - Virus spreads to Phoenix
  - Foreign cities offer to become responders
- President is pressured by prominent families to accept aid from foreign countries
- American production plummets
  - EU announces moratorium on US-made products for 12 months

Fifth Week

- US becomes 2nd World Country
- Options
  - Red team never announces: don t care
    * Red team takes over US industrial production
  - Red team never announces: President and cabinet resigns
    * Balance of power shifts to more favorable group in Congress
  - Red team announces who they are and conditions for surrender
    * Control of government
    * Or co-opts President

Scenario 1

- HOW TO ATTACK CONUS
  - (All of this is based, on the concept of "developing globalization")
  - Use "a" multi-national corporation as the aggressor
    * A la Krupp and/or Daimler-Chrysler
    * The corporation is the cover for our amorality
  - Create (or exploit) a natural disaster
  - Use position in transportation industry and products
    * "Created" traffic accidents to confound response
    * Create, or corrupt, national data bases and systems (for distribution, etc.)
    * Disrupt the wheel transportation (big truck) system to prevent distribution of food and other commodities
    * "Automate" how to do it so that it is obvious to no one but us
  - Corrupt media and network
  - Prepare (IT Phase)
    * Disinformation and Rumors
      - To advance, or counter counter, our purposes
      - Corrupt/bend CNN, Reuters, AP, etc.
      - Since "anyone, anywhere" can be a reporter use our people to report "what" we want reported
      - Tele-presence spoofers and avatars
    * Economic
      - We provide transportation (Chrysler)
    * Earthquake
      - Cause (or wait for) one (or more) in Denver and LA
      - "Turn" blame on US government for causing it by weapons testing (use avatar)

        Who apologizes for having done it

Scenario 1 (Continued)

- HOW TO ATTACK CONUS
  - Prepare (Damage/Kill Phase)
    * Overload the system and cause employment of military assets to handle "crises"
    * Contaminate/block major traffic routes in key areas
      - Corrupt data needed to assist in decontamination and recovery
    * Give impression of major terrorist activity
      - Involve RC forces/FBI/FEMA/SBA
    * In IT war
      - Corrupt "some" (not all) critical data (blood supplies, and other) needed to handle crisis
      - Interfere with the crisis C2 organizations, facilities, and equipment
  - Attack
    * Employment of Bio weapons/agents
      - Venovo virus 5-10 day latency
      - Disperse by using public transportation
    * Transportation portion of response is compromised
    * Telemedicine portion of response is compromised
    * Media spoofing creates confusion and distrust
    * Miami is a "red herring"
  - Done to reduce US to a non-competitor in order to make money
    * By definition have to consider what this will cost
      - "Go/No Go" decision will be profit based but may have other reasons also
  - Technologies Used
    * Minimum Human Maximum Robotic/Automated Involvement
      - 5% Human 95% Automated
    * Maximum deniability
    * Minimize costs/dual use of means
    * Take advantage of natural/artificial disasters
      - Confusion over who is "Red"

Participant Listing
July 2000 Conference
Dartmouth College, Hanover, New Hampshire

Ken Alibek, MD, PhD
Chief Scientist, Hadron, Inc./President, Advanced Biosystems, Inc., Alexandria, Virginia

Michael Ascher, MD
Chief, Viral and Rickettsial Disease Laboratory Branch, Berkeley, California

George Baer, PhD
Chairman, Strategy and Policy Department
Alfred Thayer Mahan Professor Maritime Strategy, US Navel War College, Newport, Rhode Island

Daniel Bilar
Research Engineer, Institute for Security Technology Studies, Dartmouth College, Hanover, New Hampshire

Mike Blayney, PhD
Director, Environmental Health/Safety, Dartmouth College, Hanover, New Hampshire

William Bograkos, DO, FACOEP
National Naval Medial Center, Silver Spring, Maryland

Jon Bowersox, MD, PhD, FACS
Associate Professor of Surgery, University of California, San Francisco
Chief of Vascular Surgery, UCSF/Mount Zion Medical Center

David Brannan
RAND, Consultant, Arlington, Virginia

Roger Breeze
USDA, Agricultural Research Services, Associate Administrator, Washington, D.C.

Charles Brush
Deputy Chief, Lebanon Fire Department , Lebanon, New Hampshire

George Cybenko, PhD
Dorothy & Walter Gramm Professor of Engineering Sciences, Dartmouth College, Hanover, New Hampshire

David Franz, DVM, PhD
Vice President, Chemical and Biological Defense Division, Southern Research Institute, Frederick, Maryland

John Gaffney
Director, Emergency Planning and Operations, UNM Health Sciences Center, Albuquerque, New Mexico

Adam Geibel
Threat Coordinator/Scenario Writer, Philadelphia, Pennsylvania

Jim Geiling, MD, FACP
Colonel, Medical Corps, Flight Surgeon, U.S. Army

Nick Giaccone
Chief of Police, Hanover New Hampshire

Ursula Gibson, PhD
Associate Professor of Engineering, Dartmouth College, Hanover, New Hampshire

Robert Gougelet, MD
Clinical Staff Emergency Physician, Dartmouth-Hitchcock Medical Center , Lebanon, New Hampshire

Bill Greenrose
Chief Financial Officer & Senior Vice President, Medical Media Systems, Inc., West Lebanon, New Hampshire

Jennifer Harper
New Hampshire Governor s Office of Emergency Management, Concord, New Hampshire

Joe Henderson, MD
Associate Professor of Community & Family Medicine, Dartmouth College, Hanover, New Hampshire

Lisa Moreno-Hix
Director of Programs, Oklahoma City National Memorial Institute for the Prevention of Terrorism, Oklahama

Richard Hutchinson, PhD
BW Improved Response Program Leader, U.S. Army, SBCCOM, Maryland

Arthur Kantrowitz, PhD
Senior Scientist Thayer School, Dartmouth College, Hanover, New Hampshire

Dan Kaszeta
Captain, Maryland Army National Guard

Robert Keating
Patrolman, Police Department, US Coast Guard Reserves, Manchester, New Hampshire

George Keros
President, Photon Physics, Concord, New Hampshire

Leland Kimball
New Hampshire Emergency Management, Concord, New Hampshire

Dennis Klinman, MD, PhD
Chief, Section of Retroviral Research CBER/FDA, Bethesda, Maryland

Peter Laporte
Emergency Management Agency, Washington, D.C.

Milton Leitenberg
Center for International & Security Studies at Marylan, College Park, Maryland

Chris Lowery, MD
Department of Medicine, Dartmouth Medical School, Hanover, New Hampshire

Charles Lucey, MD, JD, MPH
Institute for Security Technology Studies, Dartmouth College, Hanover, New Hampshire

Tracey McNamara, DVM
Head, Department of Pathology, Wildlife Health Sciences, Bronx, New York

Emmanuel Mdurvwa, MPD, PhD
State of New Hampshire Department of Health & Human Services, Concord, New Hampshire

John Modlin, MD
Professor of Pediatrics and Medicine, Dartmouth Medical School, Hanover, New Hampshire

Lt. Col Scott Moore
Advanced Systems & Concepts Office/Defense Threat Reduction Agency (DTRA), Ft. Belvoir, Virginia

Jose Montero
State of New Hampshire Department of Health & Human Services, Concord, New Hampshire

Frank Moran
Hanover, Police Department, Hanover, New Hampshire

D arcy Morgan
Institute Program Manager, National Institute of Justice, Washington, D.C.

Randall Murch, PhD
Director, Advanced Systemsand Concepts Office, Defense Threat Reduction Agency (DTRA), Ft. Belvoir, Virgina

Carolyn Murray, MD
Dartmouth-Hitchcock Medical Center Occupational/Environmental Medicine, Lebanon, NewHampshire

Michael Myjak
Vice President, R & D and CTO, The Virtual Workshop, Inc., Titusville, Florida

John Nachodsky, PA
Telemedicine and Physicians Assistant, Private Consultant, La Crescent, Minnesota

Andy Ogielski
Senior Scientist, Institute for Security Technology Studies, Dartmouth College, Hanover, New Hampshire

Walter Perry
Senior Operations Research Analyst, RAND, Arlington, Virginia

Michael Powers
Research Associate, Chemical and Biological Arms Control Institute (CIABC), Washington, D.C.

Judith Prewitt, PhD
Visiting Research Professor of Engineering, Dartmouth College, Hanover, New Hampshire

Mike Reynolds
Research Scientist, US Army Cold Regions Research & Engineering Laboratory, Hanover, New Hampshire

Joseph Rosen, MD
Associate Professor of Surgery, Dartmouth College, Hanover, New Hampshire
Dartmouth-Hitchcock Medical Center, Lebanon, New Hampshire

Paul Roth, MD
Associate Vice President for Clinical Affairs, Health Sciences Center
Dean, University of New Mexico School of Medicine, Albuquerque, New Mexico

Daniela Rus, PhD
Assistant Professor of Computer Science, Dartmouth College, Hanover, New Hampshire

Richard Scribner, PhD
Acting Director, The Institute for Security Technology Studies, Dartmouth College, Hanover, New Hampshire

Barbara Seiders, PhD
Batelle, Pacific Northwest National Laboratory, Richland, Washington

Brian Sullivan
Former National Defense University (NDU), Vienna, Virginia

John Sutton, MD
Director of Trauma Services, Dartmouth Hitchocock Medical Center
Prof. of Surgery, Medical School, Dartmouth College, Hanover, New Hampshire

William Zinnikas
Special Agent FBI, New York Joint Terrorism Task Force, New York City, New York

Raymond Zilinskas, PhD
Senior Scientist, Ctr. for Nonproliferation Studies, Monterey Institute of International Studies, Monterey, California

David Zeltzer, PhD
Chief Technical Officer, Fraunhofer Center for Research in Computer Graphics (CRCG), Providence, Rhode Island

Jian Zhao
Digital Security Tech, Center for Research in Computer Graphics (CRCG), Providence, Rhode Island

Participant Listing
September 2000 Conference
Washington, D.C.

Matt Chapman
Supervisory Special Agent, FBI, Washington, D.C.

Lewis Duncan, PhD
Dean, Thayer School of Engineering, Dartmouth College, Hanover, New Hampshire

David Franz, DVM, PhD
Vice President, Chemical and Biological Defense Division, Southern Research Institute, Frederick, Maryland

Robert Greenberg
Senior Vice President, G&H International Services LLC, Washington, D.C.

Jerome Hauer
Assistant Vice President, SAIC and Associate Director, Center for Counterterrorism, Washington, D.C.

J. Krister Holladay
Office of Congressman Saxby Chambliss, U.S. House of Representatives, Deputy Chief of Staff, Washington, D.C.

Richard Hutchinson, PhD
BW Improved Response Program Leader, U.S. Army, SBCCOM, Maryland

CDR Shaun Jones, MD
Chevy Chase, Maryland

Takeo Kanade, PhD
Professor Cargnie Mellon University, Director, The Robotics Institute U.A.

Peter Laporte
Emergency Management Agency, Washington, D.C.

Charles Lucey, MD, JD, MPH
Institute for Security Technology Studies, Dartmouth College, Hanover, New Hampshire

Anne Mohnkern Renshaw
Consultant, Weapons of Mass Destruction Strategic Plan, Emergency Management, Washington, DC

D arcy Morgan
Institute Program Manager, National Institute of Justice, Washington, D.C.

Rapheal Perl
Senior Analyst, Congressional Research Service, Washington, D.C.

William Raub, PhD
Deputy Assistant Secretary, Department of Health and Human Services, Washington, D.C.

Joseph Rosen, MD
Associate Professor of Surgery, Dartmouth College, Hanover, New Hampshire
Dartmouth-Hitchcock Medical Center, Lebanon, New Hampshire

Craig Watz
Special Agent FBI

William Zinnikas
Special Agent FBI, New York Joint Terrorism Task Force, New York City, New York

Conference Summary

Prepared by
Charles Lucey, MD, JD, MPH

Emerging Threats - Biological Terrorism
A Technology-Based Threat Assessment Workshop
July 7 - 9, 2000

Principal Investigator: Lewis Duncan, Ph.D., Dean, Thayer School of Engineering
Chairman & Organizer: Joseph Rosen, M.D., Dartmouth Medical School

Purpose

- Assess the Present & Future Threat from the Use of Biological Weapons and Cyber Attacks by Terrorists, and to Help Better Prepare for such Catastrophic Events

Scope

- Broad-based Threat and Action Assessment Involving a Range of Technical and Other Professionals

Anticipated Results

- Clearer Threat Assessment
- Refined Key Research and Action Issues
- Recommendations for Governmental, Public Health, & Other Organizations

Disclaimer: The opinions expressed are personal and are not attributable to any group or organization unless explicitly expressed.

Introduction

This executive summary is written in conjunction with the other project executive summaries to acquaint and inform, with brevity and minimal overlap. Where white papers or web resources are referenced, the reader may delve deeper, as he or she may wish.

Friday morning

Richard Scribner, Ph.D., Acting Director, ISTS, opened the meeting. He welcomed the conference and briefly reviewed the history and mission of ISTS, inviting conferees to approach him for more information. He then introduced Joseph Rosen, M.D., as the Conference Director. Dr. Rosen welcomed the attendees and pointed out the significance of the conference s mission to peer into the future and help the United States set research priorities regarding emerging biological threats. Dr. Rosen introduced the morning s first panel.

Brian Sullivan, Ph.D. (writer, consultant, former professor at the Naval War College and the National Defense University) was the first of two speakers for the Threat Panel Discussion. Dr. Sullivan stated his belief that acts of terrorism are frequently found in history and armed conflicts. The United States had episodes of tar and feathering British tax collectors before the Revolutionary War. This caused painful burns, meant to intimidate in order to accomplish a political end. Brian reviewed how the Irish Republican Army sought to use terrorism to intimidate and to cause martyrs for the populace to revere. In response, the British sought to jail rather than kill terrorists. The extent of the British desire for good public relations may be seen in their policy not to chase terrorists into Ireland during hot pursuit.

Brian Sullivan then discussed how coordination and commensurate response might be very complex. He raised the issue of what level of attribution is necessary before retaliating against a state sponsor, asking what type of response would be justifiable. He stressed how counterterrorism could be a victim of its own success; the need for prevention without publicity that could lead to the unfortunate result of the public discounting the need to prepare for future acts. Why are we a target? Dr. Sullivan believes it is our power, and the resentment it causes.

Barbara Seiders, Ph.D. (Pacific Northwest National Laboratory) then reviewed the nature of biothreats. While her talk was mostly on viable organisms, she pointed out that biological toxins are potent and easily isolated. They fall under both chemical and biological weapon conventions. Dr. Seiders discussed her use of beer-making equipment, bought at a local store, to research the production of these agents. They are cheap and easy to produce. She found that they don t require sophisticated equipment or expertise. Many materials and equipment have a dual purpose, with use in the food or medical industries, making their control difficult. The first sign of attack can take days to detect. They can be difficult to detect in the environment in the absence of an explosive dissemination.

A couple of points were brought up in the discussion following these presentations. There was a discussion of the differences in response to chemical and biological incidents by first responders. The point was also made that public health personnel may be first responders to biological attacks that have a delayed onset of symptoms. There was also a discussion of how modern treaties apply to nations, but may not technically apply to unrecognized countries, such as Afghanistan.

The second threat panel combined talks on biothreats and cyberthreats. Raymond Zilinskas, Ph.D. (Monterey Institute of International Studies), reviewed his white paper, "Possible Terrorist Use of Modern Biotechnology Techniques." This paper reviewed a collaborative effort of the National Defense University (NDU) and Monterey Institute to assess the impact that scientific advances may have on biological terrorism for the next five years. This panel reviewed major areas of advances and concluded that there was no probable, practical threat over the next 5 years from these advances. For many of the advances, the scientific concept of pleiotropism is a major obstacle. This is the creation of unwanted side effects when altering nature to achieve a desired effect. A single gene may influence several distinct and seemingly unrelated phenotypic expressions, making genetic manipulation quite complicated due to unexpected results.

Another point that many books and Dr. Zilinskas make is that the manufacture of dry powder aerosol is the main barrier to using a biological organism to kill many people. Meteorological factors are also a complicating factor, which for example, cause 80% of scientific tests attempting to study this to be scrubbed. A second issue that Ray raised in his paper was how terrorists might be hindered by limited ability to field test their discoveries. This leads to the question of whether we would detect and diagnose failed tests or attacks as such.

Dr. Zilinskas presentation stimulated some discussion. Milton Leitenberg believes that it is misleading to overestimate the scientific capabilities of terrorist groups. In the many studies in which he has participated, or reviewed, there is no evidence that expertise in biological weapons has been obtained by terrorists. However, Leitenberg did concur that, if biological terrorism did happen, it would be catastrophic. He also argued that the conference kept slipping into using assumptions about what international states could do, rather than the more limited abilities of most terrorists.

Dr. Rosen wished to emphasize the question, "Is it possible?" Not, "Is it likely, or probable?" He emphasized that the mission of this conference was to help better prepare for such catastrophic events.

Leitenberg insisted that it is essential for the United States to take a strong stance to discourage terrorist acts. From a public relations perspective, Milton believes that overstating risks will not contribute to constructive changes. He reiterated his perspective later, serving on the Friday night, public discussion panel.

Dennis Klinman, M.D., Ph.D., called genetic engineering "child s play," in today s modern lab. Dennis points to incredible advances over past ten years and the good number of graduate students familiar with them. When challenged about the practicality, he replied with this example: take the animal host of Respiratory Syncytial Virus (RSV), infect the animals to select the most virulent mutants, repeat this process every three months with the selected organisms, and, quite soon, one will have a biological WMD.

Michael Ascher, M.D. (Chief, Viral and Rickettsial Disease Laboratory, California Department of Health Services) said that while he was aware of historical evidence of the difficulty the U.S. had with researching biological weapons, modern medicine and recent public health outbreaks illustrate the present danger that we face. He emphasized the importance of preparing the public health infrastructure. Mother nature can accomplish many tricks, for example, HIV and other recent infections demonstrate new threats and evolution to avoid the body s natural defense. Looking into the future, we may one day be able to vaccinate through treated breakfast cereal. Dr. Ascher could foresee the release of drug resistant infections by terrorists to challenge the health system. Pneumococcus and tuberculosis (TB) are examples of infectious diseases currently kept in check, which could be major challenges with increased drug resistance. Other recent virus outbreaks -- Ebola, yellow fever, hantavirus, etc. -- raise concern as biological threats. Dr. Ascher cited the threat of imported cases from abroad, which demonstrates the importance of a vigilant, prepared public health structure to detect and fight disease.

Dr. Ascher is a proponent of strengthening public health systems to fight natural and terrorist acts (dual purpose use). He pointed out that a little bit of flu can close all hospital beds in San Diego. Dr. Asher mentioned the difficulty of differentiating background (natural patterns of illness) from emerging infections or even terrorist acts, using pathogenic, diarrhea causing, E. coli as an example. Smallpox is the major threat for spreading serious illness, in his opinion. He stated that imported food is not inspected for pathogens, and has had associated outbreaks. An agricultural terrorist act, such as foot and mouth disease, could mean economic disaster.

Roger Breeze, USDA, spoke about two recent instances that his agency was asked to investigate abroad to determine if the outbreaks were natural versus terrorist. Through genetic analysis and other research techniques, they were reasonably certain that one was natural and the other human-made. There was further discussion about the importance of determining origin so that attribution could be determined and then retaliation planned.

George Cybenko, Ph.D., ISTS, lectured the audience in his breezily, entertaining fashion, on how a cyberthreat could be combined with a biological threat for a synergistic attack. Using a PowerPoint presentation to show Internet cable systems across the world, he reviewed how traffic flows on the Internet and its vulnerabilities. George discussed how a terrorist might overload the system and how emergency response teams may need to lay down new cable to meet demand.

There was some discussion over comments by Bill Zinnikas (FBI), regarding the NYC World Trade Center bombing that nearly severed the ATT cable lines (voice, data, and Internet) for the east coast. There was also some talk about the need to shut off cable access for news media to free up broadband for emergency response. Andy Ogielski, Ph.D. (ISTS) pointed out that there were networking challenges and that the people involved in running some of the telecommunication networks were inexperienced. System reliability and capacity were vulnerable.

Friday s lunchtime presentation

Richard Hutchinson, Ph.D. (Biological Weapons Improved Response Leader, Soldier and Biological Chemical Command) gave a two-part presentation on threat variables and threat response that was informative and thorough. Much of this information can be seen in the web-posted PowerPoint slides, white paper, and reprint (www.engineering.dartmouth.edu/~ethreats/). Dr. Hutchinson has been part of a high level, federal effort to develop a response model or template for biological terrorism preparation.

A key idea that Dr. Hutchinson championed was a Command & Control (C&C) simulator that allows modeling of response components to see how all of these might work together. The simulation would also provide a tool to evaluate and improve these concepts. Dr. Hutchinson stated that we are physically testing and modeling components of the biological weapon (BW) response template that could be used by cities across the U.S. To perform a field test to demonstrate such a comprehensive, system seems almost impossible. Thus simulation is needed to test a BW response system at the strategic level. Dr. Hutchinson mentioned there is beta testing of automating the BW response template at the city level through the RAMS (Response Assets

Management System) computer system. This beta testing has been funded for 5 sites at present and takes two weeks to customize for each city. A much broader, more sophisticated system would be needed to link the cities and other assets together. Dick indicated his strong belief in the need for future research and development in this area.

Friday afternoon panels

The response teams from New Hampshire, New Mexico, and Maryland gave their insights for the afternoon s first panel discussion. New Hampshire is comfortable with the present Command and Control structure. They can activate their command and control center within 15 minutes of being alerted to a disaster situation.

The two members of the Maryland National Guard Rapid Response Team, Bill Bograkos, D.O. (Lieutenant Colonel, Flight Surgeon) and Daniel Kaszeta (Disaster Preparedness Advisor, White House Military Office) stressed the following in their white paper and presentation: (1) build appropriate infrastructure to equip response; (2) the Crisis Management Planning cell is a multidiscipline team of people who must be ready to coordinate, communicate, and form an organized team (otherwise we will again see crisis, chaos, and confusion); (3) in comparing the three states presented today, appreciate not only the geographical differences but also that the threat analysis could be different; and (4) the model to apply is the U.S. Interagency Domestic Terrorism Concept of Operations Plan (a copy of which they shared in reprint form). They are also confident in their area planning and preparation.

Paul Roth, M.D. (Dean, University of New Mexico, School of Medicine) led the team discussion for his state, reviewing some of the topics found in his white paper. They reviewed their collaboration with Los Alamos National Laboratories, Sandia National Laboratories, N.M. State Department of Health, and Lovelace Respiratory Research Institute to research new technologies, implement new population surveillance (via real-time reporting of E.R. complaints that may be sentinel events), and to provide training of physicians and first responders. Paul stressed the very real danger of the current threat and pushed the concept of partnership among federal, state, and private entities to mount a meaningful response strategy.

There was a good discussion with Peter LaPorte (Executive Director, Washington, D.C. Emergency Management Agency) providing animated leadership. Peter s main point was that the response teams must share common training and communication skills. In his experience, the public health people don t speak a common language with command and control (C&C) personnel until they learn to understand one another through interaction and training.

The Response Technology Panel began with Mike Myjak (The Virtual Workshop, Inc.) reviewing how military technology and costs have made it cost-effective for the development of modeling and simulation (M&S) systems to improve training. The effectiveness of these systems was demonstrated convincingly in the Gulf War. MEDical simulation NETwork (MEDNET) is a proposal to develop similar technology to apply to bioterrorism planning, training, and C&C implementation. His paper provides many of the technological details which he stated are already in existence, and ready to be applied. The system could be useful for combat, natural disaster, and other training.

John Bowersox, M.D., Ph.D. (University of California, San Francisco) gave an overview of Telemedicine and how its present acceptance is limited to niches like prison or military medicine by social and market (reimbursement) forces, rather than technological concerns. In the future, informatics, the widespread use of computers and the Internet, and real improvement in patient care will lead to further acceptance. Dr. Bowersox believes there will always need to be a human touch behind telemedicine and robotic surgery. Dr. Bowersox singled out neurosurgery as one area that this technology is currently impacting by improving patient care. Remote medical care, training, testing, and supervision are all feasible uses of this technology.

David Zelter, Ph.D. (Fraunhofer Center for Research), reviewed how computer visualization technology can contribute to detection through the use of sensors and monitoring. Situation awareness requires systems to monitor data and give alerts, filter events from background, constantly be data-mining to discover emerging threat patterns, and to utilize artificial intelligence (AI) stratagems to test the hypothesis, "Is an attack underway?" David addressed the challenge of how data interacts with humans making decisions that are critical, such as those affecting nuclear reactor disasters, recently. Decision-centered visualization is an interactive information architecture ergonomically assisting human thinking and analysis.

The panel on threat protection for biological and cyber threats had Dennis Klinman, M.D. (immunologist) talk further about the growing ability of scientists to select virulent organisms through natural selection and then modify them with variable genetic code that can be changed easily to defeat vaccine development. Dr. Jian Zhao presented his white paper on "mobile code," which is covered in our white paper section. Mobile code refers to code that is transferred to a computer chip/system, via wire or wireless transmission, as instructions or data to change the behavior of the instrument or robot. There are security concerns that terrorists could exploit or shut down our power and communication networks by attacking this instruction code.

The panel on nanotechnology, robotics and genetic engineering featured scientific presentations by three Dartmouth College professors. Ursula Gibson, Ph.D., described nanotechnology as engineering at the molecular level using physics, chemistry, and biochemistry to make a machine that can function at a molecular level. Daniela Rus, Ph.D., reviewed her work with robots that can assemble and operate in different modes while using identical robotic parts, like a Lego set. Chris Lowery, M.D., reviewed the remarkable progress of genetic engineering in attempts to treat human disease, emphasizing that this technology could be used for offensive or defensive weapon development.

Friday night address with panel discussion, public invited

Dr. George Baer, Chairman, Strategy and Policy Department, U.S. Naval War College, welcomed the public and spoke on, "Is the American Public Safe from Bioterrorism?" Dr. Baer stated that there is no certain answer to this question. Public awareness must not become public panic. Because there is a possibility of some attack, or some social disaster, there is an absolute need to prepare. Dr. Baer asked, what are the social costs of public safety? Consider the New

Hampshire state motto, "Live free or die." Will society trade freedom for security? How does one balance the two?

Does a potential terrorist have social rights? Should a terrorist be treated by standard criminal process and procedures, or, should terrorists be subject to vigorous counterterrorist measures that may abrogate those terrorists rights? If urgent intelligence were needed, should torture be used as an effective means of reflecting the community's moral authority in order to protect itself from more terrorism?

The key to all counterterrorism is timely and accurate intelligence. This may require intrusive information collection by more powerful governmental agencies. This may impose significant restrictions or even violations of what we think it means to "live free," that is to our civil liberties and perhaps even our constitutional rights. This could affect our rule of law, our right to privacy, even the fabric of our "open society." Dr. Baer asked us if we consider Bioterrorism to be enough of a threat to national security that we would decide to sacrifice some freedom in the face of this threat? Or would we choose to sacrifice the liberty and safeguards, which we guarantee to all citizens until, and unless, they are proven guilty? Would we allow torture and other violations of due process constitutional guarantees that could protect an innocent terrorist, rather than sacrificing freedom for all?

Dr. Baer stated that it is from discussions and debates such as this one that society establishes political values and maintains cohesion. Wise political leadership can aid this process, in combination with good information gathering and our democratic election process. We will have to decide how much is a society willing to live "less free" to prevent death. Dr. Baer concluded by stating that the answers to these questions depend ultimately on public awareness, on results of a "live free or die" debate, and value judgments discussed above. With these answers, politicians, police authorities, government agencies, and our military can plan intelligence gathering, preemptive action, and response strategies.

Dr. Ken Alibek provided a broad and comprehensive review of bioweapons. He discussed his personal experience in the Russian bioweapons program. Central to his discussion was the nature of individual agents that have been developed and can be developed in the near future. He discussed the nature of the agents and how the specific weapons are classified. He also discussed techniques to modify agents from their natural state to a more virulent form to optimize delivery as a weapon. He also discussed examples of a series of known agents and how they can be weaponized further. Dr. Alibek discussed how these agents can be delivered to their targets, and how they would be spread throughout the targeted population.

Saturday, July 8th, 2000

The participants were divided into three groups, with balanced interests and expertise, to develop timelines and responses, using present technology, for the following, abbreviated scenario. At Dartmouth College, students begin having flu-like symptoms and report both to the college infirmary and to local hospitals. How would you decide if there was a terrorist attack, how would you handle forensics, and what would be your response timeline as students start dying from a confined space biological agent release? Each group would agree upon a response presentation to make to all conference participants, with the help of expert facilitators who circulated among the groups.

Each group allowed its members to use their expertise to work out a plan and timeline. Group 1 discussed the following response elements. How would Dartmouth College and Hanover, N.H., deal with the worried well and avoid panic? How would the campus and the community function under such stress? They postulated that the local medical response would be overwhelmed and that antibiotics would need to be imported. They foresaw a need for good communications between different provider systems that may be operating on different forms of technology. They predicted that many students would flee the outbreak while locals would hesitate to leave. Group one felt there would be trouble making a timely diagnosis with present technology. With local first responders becoming quickly overextended, they saw a need to identify and activate relevant state agencies. They felt forensics would be difficult. Eventually there would be a need to transport patients to other state hospitals and intensive care units.

Group Two agreed with Group One that it would be difficult to identify this initially as a terrorist act or to make a diagnosis early. They expressed concern about a lack of local stockpiles for vaccines, antibiotics, and other protective items. They felt that isolation measures should be instituted to prevent possible spread, and discussed strategic concerns regarding local quarantine, with two interstate highways and Canada nearby. They postulated that campus Internet connections would allow cameras to transmit live from many locations to news media. These transmissions could hog bandwidth and force officials to ask that the media access be blocked on the system. Group Two felt a local, on-site command and control operations center would need to be set up. Most felt that local police and other officials would remain at their posts while others felt that they would probably flee, forcing military units to replace their functions. They wondered about whether a terrorist would issue a statement and how that might impact a response plan. They also wondered about copycat false claims and how the op center could evaluate other threats.

Group Three decided that early diagnosis was the most important means of intervention. They charted a flow diagram with 20 or more boxes representing local, state, and federal resources that would need to be contacted and coordinated. While many early patients might be treated as ordinary viral flu cases not requiring antibiotics, they postulated that some sentinel cases (patients with concurrent serious medical conditions) would be more quickly and thoroughly investigated (tests and cultures) resulting in an infectious diagnosis of plague within 4 to 5 days. Group 3 felt that education and awareness by medical personnel could make a real difference but didn t know if local physicians had taken any special training for biological attacks. They felt that due to the seriousness of the illness and the small Dartmouth College community, physicians would realize within 24 hours of the first sick student that an epidemic of some sort was occurring. Group 3 theorized that 5 to 10% of the population may be on antibiotics at any time and be protected from some infections. They theorized that some patients with flu symptoms would receive antibiotics early in the disease while others would be treated with antivirals, which would not be protective. They identified 7 negative pressure rooms for protective isolation available locally. While this small number of rooms initially would be overwhelmed, they felt that once prophylactic antibiotics were started, containment would be less of an issue. They felt that hotels and dorms could be converted to patient wards.

In the discussion that followed the small group presentations, a timeline was established for identification of the agent for 5 to 10 days post attack. Suspicion of terrorist attack would be then quickly aroused by the unique infection -- plague. Identifying the site of the attack would take some good epidemiology to show where the agent was released. The terrorists could be difficult to identify and be attacking other sites while the investigation proceeded. Another point made by some participants was how different biological incidents are from other disaster planning. Some felt that many parts of response planning were similar while others sided with the unique needs for vaccines, medicines, and infection control measures. There was a sense that local responders would have difficulty with coordinating the response. Some worried that a significant number might flee or refuse to perform assigned roles, requiring military units to substitute, possibly exposing more people to deadly organisms. It was noted that the community would experience chaos.

At noon, Tracey McNamara, D.V.M., recounted the West Nile Virus epidemic, which caused New York City officials to wonder if they were under attack in the summer of 1999. Her very detailed presentation gave nearly a day-by-day, month-by-month account of the challenge she and her colleagues faced in N.Y.C. When workers at the Bronx Zoo first noticed dying crows and other birds, it was a struggle to make the correct diagnosis. No secure veterinary labs are available comparable to the Level 4 lab that the CDC (Center for Disease Control) maintains. Necessary diagnostic tools such as electron microscopy had to be begged for and waited on. Communication barriers required daily conference calls with many different speakers. A misdiagnosis was made of another mosquito borne virus. Dr. McNamara believes that there just aren t enough resources devoted to veterinary pathology laboratories in this country, especially in light of the fact that they played a central role in detecting and diagnosing this virus, which had not previously been known to be on the east coast.

Saturday afternoon was the whole group s opportunity to respond to another scenario, set in 2005, with several participants grouped together to act as the Federal Bureau of Investigation (FBI), Food and Drug Administration (FDA), Federal Emergency Management Agency (FEMA), and so forth. They were instructed to think how advanced technology might be useful if employed. The local response group reported on the scenario, in real time mode, as time passed from the moment that Hanover s Chief of Police learned that 4 similarly ill patients had been treated in the local ER, with the staff believing that it was smallpox clinically. The Chief immediately placed a call to the governor s office to request assistance.

The Governor s office contacted the CDC in Atlanta. The CDC directed samples to be secured and transported to Atlanta by a field representative trained to handle such dangerously infective materials. The FBI was notified to become the lead agency for possible terrorist incident, given that smallpox was suspected. FEMA was notified, vaccine mobilization was done, and emergency operations planning undertaken. CDC epidemiologists started determining where the infected patients (cases) have been and with whom they have been in contact.

The decision was made at the site emergency operations center (Hanover Police Station) to place the hospital under protective quarantine for public health reasons. The White House issued a press statement that all necessary measures were being taken to both protect the public health and to determine if a terrorist incident had occurred.

In Hanover, the Police Chief was now awaiting for National Guard forces to arrive. The local radio and TV stations were providing education and reassurance. Further consideration was being given to how to deploy police and fire department assets to contain the infection. While there were only 4 suspected cases of smallpox, it was decided that this could be a national emergency requiring an interstate quarantine. The Attorneys General for both VT and NH cooperated to achieve this.

By 24 hours after the Police Chief had been notified, the worried well and the news media had completely overwhelmed the 911 and commercial communication systems. There are concerns about distributing food and water to families confined to their homes.. State police has closed the roads and airport. The CDC is coordinating additional medical supplies. Their Level 4 Lab is utilizing PCR (polymerize chain reaction) and EM (electron microscopy) to study their samples. The preliminary diagnosis is pox virus. Their epidemiology officers have found that all victims ate at Thayer dining hall, 8 to 9 days earlier, but need more time and testing to definitively state this was the infection site.

The Department of Defense is mobilizing additional resources for command and control. The FBI has started to investigate the backgrounds of the sick patients and other suspicious visitors for leads. They are also helping the CDC determine where the cases have been and who their contacts have been. The vaccines arrive but there is confusion on how to organize vaccination efforts. The CDC personnel begin training local persons on how they want the vaccine administered. They have told the White House that they need to contain this now, as it would take 6 months to make enough vaccine to protect the entire country.

The U.S. Attorney General has briefed the President on the range of emergency powers he may exercise, including restricting immigration and use of quarantine for public health protection. As Hanover approaches 48 hours since the emergency started, interactive video links and telesupport from remote sites are set up and staffed. Hanover has not received any more food and the National Guard needs more resources. The CDC is working on genetically identifying the virus and on containment strategies. National healthcare providers are briefed and their assistance requested. Experts at the United States Army Medical Research Institute of Infectious Diseases (USAMRIID) are requesting that samples and data be dispatched for Fort Detrick, in Frederick, MD, to assist the CDC.

As we enter the third 24-hour period of the crisis, the President is notified that more smallpox cases are being diagnosed and that there is more concern that this is a terrorist attack that may be complicated by other attacks. No group has claimed responsibility. In Baltimore, there are two possible additional cases, which the CDC is investigating. The National Guard and the Department of Defense (DOD) are further developing logistics coordination, deploying immunized medical staff, providing security, and assisting with civil affairs.

In Hanover, residents are quarantined at home, containment of infected individuals is enforced, and there is need for more protective suits. The CDC is working on national guidelines should the epidemic spread outside of current areas. The Maryland National Guard has been put on alert. Available Internet communication bandwidth has suffered several blackouts due to heavy demand and denial of service episodes, suspected as cyberattacks. Communication companies are attempting to manage networks but appear somewhat hampered by young, inexperienced, engineers and directors.

New Hampshire has issued a call for assistance from other states. Volunteers, led by the Maryland National Guard, are ready to operate telemedicine remote hospital wards. Once the advanced MASH (Mobile Army Surgical Hospital) units are deployed, they will be remotely supported by 500 volunteer Maryland physicians and 1500 nurses, plus other support staff, using a staffing ratio of one physician and three nurses per 10 critically ill patients. With telemedicine, telesurgery, and advanced robotics, ICU care can be extended to over 15,000 potential victims, while protecting medical personnel from exposure to the biological attack. Local civilians, who have already suffered exposure, are asked to volunteer for their help in operating the MASH units. Less ill patients can be telesupported in their homes via Internet 2 bandwidth.

At one week out, 30% of the Hanover population is deceased with the number of deaths increasing each day. The population doesn t believe the immunizations to be protective. The CDC and USARMIID now believe that this is a monkey pox, biologically altered with smallpox, a deliberate act of terrorism. It does not seem to be as contagious as smallpox. They are unsure how to make the natural smallpox vaccine more effective. They estimate it could take 6 months to develop a new vaccine. They are performing susceptibility testing for the limited antiviral compounds currently approved for other indications.

By day 9, the Hanover area is passing through a secondary cycle of disease. The ranks of the caretakers and their medical supplies are depleted. Some inhabitants, principally students, are feared to have sneaked away from the area. Only families fully quarantined from the community are untouched by illness, staying indoors in their homes. The military has fully taken control of police and emergency services and is suffering some casualties, despite previous smallpox vaccination and investigational prophylaxis with antiviral medicines.

In Maryland, there are currently 17 infected patients. The airports are closed, the National Guard has been mobilized, and the worried well are flooding hospital emergency rooms with flu symptoms and minor rashes. While the CDC has confirmed the second epidemic center, two other suspected outbreaks have been declared improbable while investigations continue.

The White House has been issuing frequent press briefings to calm people while urging citizens to be aware of any suspicious activities. They have agreed with Canada to close their mutual border as a precaution while Mexico continues to monitor the situation. There is a sense of terrible national crisis. The fear is widespread and almost palpable. The European Union is expected to ban travel and commerce. They are setting up 30-day quarantine procedures, though no one knows how long quarantine is needed to prevent transmission.

The good news is that, although there have been isolated confrontations between citizens demanding medicine or vaccine and aid workers, the populace has remained calm. The country has rallied around the executive branch s vow to find and prosecute the terrorists, promising retribution to any country caught aiding them. Congress is meeting in special session, passing emergency legislation for the FDA and other agencies to meet the urgent demand to find new vaccines or medicine.

The role playing was stopped to allow some scenario review. A majority felt that this cooperative command and control structure was a challenge to operate. Coordination between state and local officials seemed strained without on site or close communication. People were forced to think and act quickly, decisively. The pressure of the uncontrolled outbreak was relentless, inducing fatigue and discouragement.

Sunday, July 9th, 2000

Dr. Joseph Rosen addressed the session. He began by referring to the Defense Science Board finding that biological attack could equal a nuclear attack in its impact on our population. Dr. Rosen proposed that it is in our national interest to embark upon a major research initiative comparable to the Manhattan project to develop a coherent strategy for terrorism and WMD defense. Response planning based upon advanced computer simulation combined with robotic technology must be developed. Dr. Rosen used the experience of the simulation scenarios performed on Saturday as an argument that the present plan for extensive cooperation between various federal and state agencies may need to be improved by a unified command structure. At present, local response would probably best be managed by military units trained for biowarfare. Dr. Rosen foresees a great need to build a strong science and technology base for biological defense. He sees the need for extensive practice and training that would engage non-DoD participants for improved civilian preparation.

Dr. David Franz of the Southern Research Institute presented the findings of his white paper (also see Recommendations Executive Summary). He stated that we do not know the limits of biotechnology either offensively or defensively. At present there are no technological solutions. We need a much deeper technological research base to find future answers. We need to find the sustained leadership necessary to find and manage a Manhattan-type initiative. This initiative would have to be coordinated across agencies, and civilian and military lines. The Department of Defense can do the research and development but we need to bring industry into the project to bring the items to market.

Intelligence procurement is both important and often difficult to implement. Much of the production machinery can be used for dual purposes. Intelligence with technological resources must be complemented with human access. There is a need for cooperative threat reduction just as we have done with the Russian nuclear program. There is a need for better threat analysis so that prevention, preparation, simulation, and response are properly planned out. The public health structure can be improved to help us deal with biological threats, and has the added benefit of improving the health of our society.

Forensics is another top priority. We must be able to dissect down to molecular level. This type of crime must be handled like any other to preserve evidence including microbial and DNA sampling. Laboratory architecture must continue to improve for more rapid detection, analysis, and treatment. Its methods of analysis will need to be validated. These investments in our capabilities will allow the president to respond to the future threats.

Medical countermeasures must be improved. This includes pre-clinical diagnosis (detection). This allows for earlier treatment and also allows us to know who was exposed. Dr. Franz believes that selective vaccines may be effective for military personnel. We can work harder on our antiviral drug program, leveraging the efforts of the pharmaceutical industry. New masks and suits are more useful for the military than for the civilian population. Dr. Franz points out that even the use of a mask requires early warning. Dr. Franz discussed the need for interagency collaboration, both horizontally and vertically. He commented that yesterday's scenarios illustrated how this can be difficult. Good information is key for good cooperation.

Educating the public and first responders must be a priority. The effort must be thought out carefully. The United States might look to the Israeli model of civilian terrorist defense for such planning. In the discussion that followed Dr. Franz's presentation, there was agreement of a need to have the will to retaliate based on reliable forensic findings. Our technology needs to be accurate enough to properly attribute a terrorist incident so that conventional retaliation can be made.

Randall Murch, Director of Advanced Systems and Concepts Office, Defense Threat Reduction Agency, addressed the panel with the following observations. This conference, like others that preceded it, has assessed the threat from biological terrorism to be real. The United States needs to consider how social engineering may be able to prevent future terrorist incidents by its own citizens. Using modern technology, there is now the opportunity to study and model terrorist groups. From such modeling, we can be better prepared to design our responses. The threat is critical. There needs to be seamless integration of information technology. Command and control centers must be able to communicate important information to response teams.

There is a need for rapid response and mobile response teams. Mr. Murch agrees that our educational resources must be better distributed. He cited a naval operation in Orlando as one resource. Early warning is imperative for effective deterrents. There must be good medical intelligence and preparation. He believes that the best defense is a good offense. Planning is entwined with education. Education then leads to better preparation. In his opinion, the public health system needs to be prepared for such a threat. Grants and funding can bring more attention to this public health need. Awareness is very important for good preparation. Mr. Murch believes that this effort requires strong leadership, though it may not quite rise to the level of a Manhattan project.

In the discussion that followed Mr. Murch's discourse, Dr. Rosen discussed some of the new technology that can be quickly brought to bear upon this problem. Robotics as response technology is now feasible. In institutions like Carnegie-Mellon, robotics research is progressing rapidly. Dr. Rosen has seen demonstrated a small, autonomous helicopter that can fly up 50 feet off the ground and accurately deliver a 1 kg package. This helicopter can be programmed with GPS (global positioning system) instructions. He foresees using robotics to help quarantine an area. His proposed simulation system relies upon hardened networks or rapidly deployed fiber-optic cable to provide communication bandwidth. Dr. Rosen believes that science has become so specialized that we lack people who can operate across specialties to create these types of response technologies.

Professor George Cybenko about computer issues. Dr. Cybenko sees command and control as radically evolving in the next few years. To illustrate this, he pointed to the bust of Sylvanius Thayer in the School of Engineering conference room. Mr. Thayer graduated from Dartmouth College and attended West Point around 1800. From there, he traveled to France to study how Napoleon commanded his troops. Napoleon required regular written reports every week. Napoleon found that this led to better management and helped avoid confrontation. This type of management came to be known as the "line staff" method. It s time for us to invent new management styles. We need to study the infrastructure of the Web to find new management techniques. The Web allows for information to be shared. Information is also dispersed on many servers. This Internet allows for new sensors (e.g., software gauges and monitors) to be programmed, for the structures to be built (infrastructure), and for us to synthesize novel ways to organize ourselves. A question was raised regarding the reliability of such a network. Dr. Cybenko answered to the effect that nobody said it would be easy, but he felt confident it could be done.

With time running out for the conference, a few last comments were taken from the participants. Dedicated communication capabilities and mobile telemedicine were described as quite desirable R&D programs. The important idea that an ounce of prevention is worth a pound of cure applies to biological terrorism response planning. There can be a lot of dual utility of systems to promote worthwhile projects such as improving public health. The conferees agreed that an advisory board would review and approve a final report, then adjourned.

For further conference information, please view our website,
www.engineering.dartmouth.edu/~ethreats/, and the white papers submitted.

The **I**nstitute for **S**ecurity **T**echnology **S**tudies is a research institute on security technology studies and is established at Dartmouth to work with the U.S. Justice Department, the National Domestic Preparedness Office, and other governmental agencies as a principal national center for cyber-security, infrastructure protection, and related counter-terrorism technology research, development and assessment. The core program of the institute is essential R&D in the area of cyber-security and enhancing information infrastructure resource protection.

President Clinton and Congress have identified this as an area of national priority. We are increasingly dependent on the Internet. Our electronic infrastructures are key in financial systems, commerce of all kinds, transportation, energy, health care, communication, government operations at all levels, and basic human service. There are thoughtless or malicious entities as hostile adversaries of the U.S. that would try to commandeer or destroy aspects of this system in an attempt to harm American security, its public or its prosperity. Recent hacker attacks and intrusions demonstrate the loss of control of or access to informational, commercial, and command and control resources that can result, and highlight the loss of confidence in such control. Research, technology development and other efforts are required to prevent future attacks, to protect critical information infrastructure resources, to effectively react to attacks, and to identify, investigate and pursue the attackers.

The institute drawing upon the strengths of Dartmouth and also in collaboration with other universities and laboratories, will study and develop technologies addressing needs in the areas of (a) threat characterization and intelligence, (b) threat detection and interdiction, (c) preparedness and protection, (d) response, and (e) recovery.

It will conduct a nationally defined and coordinated agenda of research, development, and technology assessment studies in the area of information infrastructure protection. The institute s activities as currently planned include a major core program focussing on

1. Cyber-security and
2. information infrastructure assurance, with additional related efforts on
3. emergent threats assessment including especially those related to cyber-security, and
4. information technology applied to preparedness and training, and a possible fifth area of
5. counter-terrorism studies drawing upon the computational and other disciplinary strengths of Dartmouth.

The work will include basic scientific and engineering research, delivery of transferable innovations and new technologies, development of prototypes and proof-of-concept demonstrations and testing and evaluation of technologies independently developed.

The institute is in the early stages of development at this time and it is premature to report on many of the details. But, we can say that

a) It will conduct and support research and development of new technologies and

methods to protect and enhance the security and robustness of our Nation s critical information infrastructures.
b) The work will include studies of information networking, computer systems, and critical information technology applications and standards, that are increasingly vital to our economic health and competitiveness, national security, and social well-being.
c) This work supports continued technology development for the threat assessment, intelligence, interdiction, prevention, response and recovery needs of Federal, State and local preparedness and law enforcement agencies, as well as private and public organizations dealing with these issues.

It is also created to have a major role in providing technical support for the National Institute of Justice (NIJ), Office of Science and Technology in service of its comprehensive agency counter-terrorism missions, and to the National Domestic Preparedness Office, the coordinating body for federal counter-terrorism programs. These efforts will include work in such areas as state and local needs, clarifying technology requirements, coordination and effectiveness, technical support for training, standards, and programmatic content, and certain clearinghouse activities.

The Institute will work collaboratively with governmental and private sector laboratories and other entites across the nation. Critical contributions to the Institute s agenda will be made from departments within Dartmouth including the Thayer School of Engineering, Dartmouth Medical School, and the College s Computer Science Department.

For further information visit our website at www.dartmouth.edu/ists.